Manuale dell’utente

BitDefender Antivirus 2010
Manuale dell'utente

Pubblicato 2010.04.19

Avvertimenti Legali

Indice

Accettamento della Licenza per utenti finali

SE NON SI ACCETTANO I TERMINI E LE CONDIZIONI NON INSTALLARE IL SOFTWARE. SELEZIONANDO "ACCETTO", "OK", "CONTINUA", "SI", OPPURE INSTALLANDO O UTILIZZANDO IN OGNI CASO IL SOFTWARE, STATE INDICANDO IL VOSTRO COMPLETO BENESTARE E ACCETTANDO I TERMINI DI QUESTO ACCORDO.

REGISTRAZIONE DEL PRODOTTO. Con l'accettazione del presente accordo, l'Utente si impegna a registrare il software, utilizzando il pulsante "Il mio account", come condizione del proprio utilizzo del Software (e ricezione degli aggiornamenti) e il diritto di manutenzione. Questo controllo contribuisce a far sì che il software funzioni solo su computer che hanno una licenza valida e che solo gli utenti finali con Licenza valida possano ricevere servizi di manutenzione. La registrazione richiede un prodotto con un numero di serie valido e un indirizzo e-mail valido per il rinnovo e altri avvisi.

Questi termini ricoprono le Soluzioni e i Servizi BitDefender per gli utilizzatori Home, incluse le documentazioni relative e qualsiasi aggiornamento e rinnovo delle applicazioni rese disponibili dalla licenza acquistata o qualsiasi servizio in accordo a quanto definito nella documentazione e ogni copia di questa.

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e BITDEFENDER, per l'utilizzo dei prodotti Software BITDEFENDER identificati sopra, che include il software e può includere supporti digitali, materiale stampato, e documentazione “online” oppure elettronica (qui di seguito designata come “BitDefender”), tutti protetti dalle leggi degli Stati Uniti ed internazionali sul copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere vincolato ai termini di questo accordo. Se non accetti i termini di questo accordo, non installare ne usare BitDefender; puoi, in ogni caso, riportarlo al tuo punto vendita per il rimborso completo dell'importo versato, entro 30 giorni dall'acquisto del quale potrà essere richiesta una ricevuta.

Se non si è d'accordo con i termini che determinano il contratto di utilizzo della licenza, non installare o utilizzare BitDefender.

Licenza BitDefender. BitDefender è protetto da leggi e trattati internazionali su copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è autorizzato, non venduto.

CONCESSIONE DI LICENZA. BITDEFENDER concede,solamente all'utente che l'ha acquistata e non a terzi, la presente licenza non esclusiva, limitata, non assegnabile, non trasferibile, non concedibile in ulteriore licenza e produttrice di royalties, a utilizzare BitDefender.

APPLICAZIONE DEL SOFTWARE. Si può installare e usare BitDefender, su quanti computers è necessario ma limitatamente al numero totale di utenti autorizzati dalla licenza. E' possibile fare una copia addizionale di back-up.

LICENZA UTENTE DESKTOP. Questa licenza si applica al software BitDefender che può essere installato su un computer singolo e che non fornisce servizi di rete. Ogni utente principale può installare questo software su un computer singolo e può eseguire una copia aggiuntiva per il backup su un dispositivo diverso. Il numero di utenti principali consentito è il numero di utenti della licenza.

PERIODO DI LICENZA. Il periodo di validità, avrà inizio dalla data in cui viene eseguita l'installazione, la copia, o quando viene usato in qualche modo, per la prima volta, BitDefender, e continuerà solamente sul computer dove è stato originariamente installato.

SCADENZA. Il prodotto cesserà di compiere le sue funzioni immediatamente dopo la scadenza della licenza.

UPGRADE (AGGIORNAMENTO). Se BitDefender è identificato come un upgrade, per usarlo devi essere stato autorizzato precedentemente ad utilizzare un prodotto classificato da BITDEFENDER come idoneo all' aggiornamento. Un prodotto BitDefender classificato come upgrade, sostituisce o complementa il prodotto originariamente installato e idoneo. Puoi usare il prodotto aggiornato esclusivamente in conformità con i termini di questo Accordo di Licenza. Se BitDefender è l' upgrade di un componente di un pacchetto di programmi software, dato in licenza come un solo prodotto, può essere utilizzato e trasferito solamente come parte integrante di questo pacchetto e non può essere separato per l’utilizzo su più di un computer.

COPYRIGHT. Tutti i diritti, titoli, e interessi derivati da o verso BitDefender e tutti i diritti di copyright derivati da o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e “applets” incorporati nel BitDefender) il materiale stampato allegato e qualsiasi copia di BitDefender sono proprietà della BITDEFENDER. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, BitDefender deve essere considerato come qualunque altro materiale protetto da copyright ad eccezione del fatto che è possibile installare BitDefender su un singolo computer conservando l’originale esclusivamente per scopi di backup o archiviazione. Non è permessa la copia o riproduzione del materiale stampato e allegato al prodotto o supporto BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui vi sia BitDefender, è necessario riprodurre ed includere tutte le note copyright in formato originale. Non è permesso noleggiare a terzi, vendere, dare in leasing, la licenza di BitDefender. Non è permesso smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire, individuare, il codice fonte di BitDefender.

GARANZIA LIMITATA. BITDEFENDER garantisce che il supporto con il quale viene distribuito BitDefender è esente da difetti per un periodo di trenta giorni dalla data in cui viene consegnato. In caso di difettosità riscontrate, BITDEFENDER, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. BITDEFENDER non garantisce che BitDefender sarà sempre privo di errori o che gli errori verranno comunque corretti. BITDEFENDER

non garantisce che BitDefender soddisferà le necessità dell'utilizzatore. BITDEFENDER CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPLICITA CHE IMPLICITA. LA SUDDETTA GARANZIA E' ESCLUSIVA E SOSTITUISCE TUTTE LE ALTRE GARANZIE, SIA ESPLICITE CHE IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIABILITA', DI ADEGUAMENTO AD UN PROPOSITO PARTICOLARE, O DI NON INFRAZIONE. QUESTA GARANZIA CONCEDE DIRITTI LEGALI SPECIFICI CHE POSSONO VARIARE DA STATO A STATO.

ECCETTO PER QUANTO CHIARAMENTE SOTTOLINEATO IN QUESTO ACCORDO, ESPRESSAMENTE O IMPLICITAMENTE, RISPETTO AI PRODOTTI, AI MIGLIORAMENTI, ALLA MANUTENZIONE O AL SUPPORTO AD ESSI RELATIVI, O A QUALSIASI ALTRO MATERIALE (TANGIBILE O INTANGIBILE) O SERVIZIO FORNITO DA QUESTI. BITDEFENDER QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITA, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, APPROPRIATEZZA PER UNO SCOPO PARTICOLARE, TITOLO, NON INTERFERENZA, ACCURATEZZA DEI DATI, ACCURATEZZA DEL CONTENUTO INFORMATIVO, INTEGRAZIONE DEL SISTEMA, E NON VIOLAZIONE DEI DIRITTI DI TERZE PARTI ATTRAVERSO IL FILTRO, LA DISABILITAZIONE, O LA RIMOZIONE DI TALE SOFTWARE, SPYWARE, ADWARE, COOKIE, E-MAIL, DOCUMENTI, PUBBLICITÀ O SIMILI, DI TERZE PARTI, CHE SI ORIGININO DA STATUTO, LEGGE, CORSO DI TRATTATIVE, COSTUMI E PRATICA, O USI DEL COMMERCIO.

DECLINAZIONE DELLE RESPONSABILITA' DI DANNI. Chiunque utilizzi, provi oppure valuti BitDefender, si assume tutto il rischio della qualità e delle prestazioni di BitDefender. In nessun caso BITDEFENDER sarà ritenuta responsabile di qualunque danno di qualsiasi tipo, inclusi senza limitazioni, danni diretti o indiretti derivati dall' utilizzo, o la consegna di BitDefender, anche nel caso in cui BITDEFENDER sia informata dell'esistenza o la possibilità che tali danni possano verificarsi. ALCUNI STATI NON CONSENTONO LA LIMITAZIONE O L' ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. IN NESSUN CASO COMUNQUE, LA RESPONSABILITA' DI BITDEFENDER POTRA' ECCEDERE IL PREZZO CHE PAGATO PER L'ACQUISTO DI BITDEFENDER. Le restrizioni e limitazioni fissate saranno applicate indipendentemente dal modo in cui si accetta di usare, valutare o provare BitDefender.

Alcuni stati non consentono la limitazione o l'esclusione di responsabilità per danni incidentali o consequenziali, per cui la succitata limitazione o l'esclusione non può applicarsi a voi.

In nessun caso BitDefender ha la responsabilità di risarcire un prezzo di acquisto più alto pagato da voi per BitDefender. Le rinunce e le limitazioni di cui sopra si applicano indipendentemente dal fatto che si accetta di utilizzare, valutare, o testare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E ESENTE DA EVENTUALI DIFETTI PROVOCATI ANCHE DALL'UTILIZZO

DELLO STESSO, E NON E’ STATO PROGETTATO NE’ DESTINATO ALL’USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTIVITA' IN MANCANZA DI SICUREZZA. QUESTO SOFTWARE NON E’ ADATTO ALL’USO IN OPERAZIONI DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE, ISTALLAZIONE, DOVE L’ERRORE POSSA PROVOCARE MORTE, LESIONI FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

CONSENT TO ELECRONIC COMMUNICATIONS. BitDefender può dover inviare avvisi legali e altre comunicazioni circa il Software e la sottoscrizione dei servizi di manutenzione o il nostro uso delle informazioni che vengono fornite ("Comunicazioni"). BitDefender invierà Comunicazioni tramite avvisi interni al prodotto o avvisi via e-mail all'indirizzo e-mail primario registrato dall'utente, oppure effettueraà Comunicazioni sui propri Siti. Con l'accettazione del presente Accordo, l'utente acconsente a ricevere tutte le Comunicazioni attraverso questi mezzi elettronici e dimostra di essere in grado di accedere alle Comunicazioni sui Siti.

AGGIORNAMENTI: accettando questo accordo, lei riconosce e accetta che il suo sistema sia utlizzato per ricevere e utilizzare aggiornamenti attraverso un protocollo peer to peer. Il protocollo non verrà utilizzato per niente altro che trasmettere e ricevere signature degli aggiornamenti BitDefender.

TECNOLOGIA DI RACCOLTA DATI- BitDefender informa che in alcuni programmi o prodotti potrebbe usare una tecnologia di raccolta dati per raccogliere informazioni tecniche (fra cui i file sospetti), per migliorare i prodotti, per fornire servizi collegati, per adattarli e per prevenire l'uso illegale o privo di licenza del prodotto o i danni causati da prodotti malware. L'Utente riconosce e accetta che BitDefender può utilizzare tali informazioni come parte dei servizi forniti relativamente al prodotto e per la prevenzione e l'arresto dell'esecuzione di programmi malware sul computer.

Accettando questo accordo, lei riconosce e accetta che la tecnologia per la sicurezza scannerizzi il suo traffico al fine di individuare eventuali malware e di prevenire i danni che questi potrebbero produrre.

L'Utente riconosce ed accetta che BitDefender possa fornire aggiornamenti e miglioramenti al programma o prodotto che vengono automaticamente scaricati sul computer.

Con l'accettazione del presente Accordo, l'Utente acconsente all'upload dei file eseguibili affinché questi possano essere scansionati dai server BitDefender. In modo simile, al fine di stabilire un contratto e di utilizzare il programma, l'utente potrebbe dover fornire a BitDefender alcuni dati personali. BitDefender informa che tratterà i dati personali in conformità con la legislazione vigente applicabile e come stabilito nelle sue Politiche sulla Privacy.

RACCOLTA DATI. L'accesso al sito web da parte dell'Utente e l'acquisto di prodotti e servizi e l'utilizzo di strumenti o contenuti tramite il sito web implicano

l'elaborazione di dati personali. Il rispetto delle normative relative all'elaborazione di dati personali, ai servizi informatici e al commercio elettronico è di assoluta importanza per BitDefender. Talvolta, per accedere ai prodotti, ai contenuti o agli strumenti l'utente dovrà in alcuni casi fornire alcune informazioni personali. BitDefender garantisce che tali dati verranno trattati confidenzialmente e in conformità alle normative relative alla protezione dei dati personali, ai servizi informatici e al commercio elettronico.

BitDefender rispetta le normative applicabili in materia di protezione dei dati ed ha compiuto i passi amministrativi e tecnici necessari a garantire la sicurezza dei dati personali che raccoglie.

L'Utente dichiara che tutti i dati forniti sono veritieri ed accurati e si impegna ad informare BitDefender di qualsiasi cambiamento di tali dati. L'Utente ha il diritto di opporsi all'elaborazione di qualsiasi dato che non sia essenziale per l'esecuzione dell'accordo e all'uso per qualsiasi scopo diverso dal mantenimento della relazione contrattuale.

Nel caso vengano forniti dettagli di terzi, BitDefender non sarà responsabile per il rispetto dei principi di informazione e di consenso, e sarà pertanto cura dell'utente garantire di aver preventivamente informato ed ottenuto il consenso dal proprietario dei dati, relativamente alla comunicazione di tali dati.

BitDefender e i suoi affiliati e partner invieranno informazioni di marketing per email o altri mezzi elettronici solo a quegli utenti che hanno acconsentito esplicitamente a ricevere comunicazioni o newsletter relative ai prodotti o servizi BitDefender.

Le politiche sulla privacy di BitDefender garantiscono all'utente il diritto di accedere, correggere, eliminare ed opporsi all'elaborazione di dati tramite avviso via e-mail all'indirizzo: juridic@bitdefender.com.

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul diritto d'autore. La giurisdizione esclusiva e la sede di decisione per qualsiasi disputa che sorga al di fuori di questi Termini di Licenza sarà in capo ai tribunali della Romania.

Nel caso di invalidità di qualsiasi previsione di questo Accordo, l'invalidità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i loghi BitDefender sono marchi registrati di BITDEFENDER. Tutti gli altri marchi registrati utilizzati nel prodotto o nei materiali associati sono di proprietà dei rispettivi titolari.

La licenza terminerà immediatamente senza notifica se si infrange uno qualsiasi dei suoi termini e condizioni. Non si ha diritto ad alcun rimborso da BITDEFENDER o da qualsiasi rivenditore di BitDefender come risultato della cessazione. I termini e le condizioni che riguardano la riservatezza e le restrizioni d'uso resteranno in vigore anche dopo qualsiasi cessazione.

BITDEFENDER può revisionare questi Termini in qualsiasi momento e i termini revisionati si applicheranno automaticamente alle versioni corrispondenti del Software distribuito con i termini revisionati. Se qualsiasi parte di questi Termini è giudicata nulla o non applicabile, ciò non avrà effetto sulla validità del resto dei Termini, che resteranno validi ed applicabili.

In caso di controversia o inconsistenza tra le traduzioni di questi Termini nelle altre lingue, prevarrà la versione inglese emessa da BITDEFENDER.

Contatta BITDEFENDER, al n.5 di via Fabrica de Glucoza, 72322-Sector 2, Bucarest, Romania, o al N. di Tel. : 40-21-2330780 o di Fax: 40-21-2330763, indirizzo e-mail: office@bitdefender.com.

Prefazione

La presente guida è destinata a tutti gli utenti che hanno scelto **BitDefender AntiVirus 2010** come soluzione di sicurezza per i loro PC. L'informazione presentata in questo libro è indicata non solo per esperti di computer ma è inoltre accessibile a chiunque sia capace di utilizzare Windows.

Questo manuale illustra BitDefender Antivirus 2010, e il processo di installazione e configurazione. Sarà possibile imparare ad utilizzare BitDefender Antivirus 2010, ad aggiornarlo, testarlo e personalizzarlo, in pratica come sfruttare al meglio BitDefender.

Ti auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritte con caratteri `monospazio`.
http://www.bitdefender.com	I link URL puntano su alcuna ubicazione esterna, su server http o ftp.
sales@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo per informazioni sui contatti.
«Prefazione» (p. xv)	Questo è un link interno, verso qualche ubicazione nel documento.
`filename`	File e directory (cartelle) vengono scritte con fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono scritte usando caratteri in **grassetto**.
`sample code listing`	Il listato codici è scritto con caratteri `monospazio`.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, offrendo alla tua attenzione informazione addizionale relativa al paragrafo corrente.

Nota
La nota è solo una piccola osservazione. Anche se la puoi omettere, la nota può provvedere informazione di valore come una caratteristica specifica o un link verso temi relazionati.

Importante
Questa richiede la tua attenzione e non è consigliato saltarla. Solitamente facilita informazione non critica ma significante.

Avvertimento
Questa è un'informazione critica che dovresti trattare con crescente cautela. Niente di male accadrà se segui le istruzioni. Dovresti leggerlo e capirlo, perché descrive qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione e rimozione. Istruzioni passo passo per l'installazione di BitDefender su un personal computer. Partendo dai prerequisiti per una installazione valida, l'utente viene guidato lungo l'intero processo di installazione. Infine la procedura di rimozione viene descritta nel caso si abbia bisogno di disinstallare BitDefender.

Iniziando. Contiene tutte le informazioni necessarie a muovere i primi passi con BitDefender. Viene presentata l'interfaccia di BitDefender e le procedure per risolvere i problemi, configurare le impostazioni di base e registrare il prodotto.

Modalità intermedia. Presenta l'interfaccia Modalità Intermedia di BitDefender.

Modalità avanzata. Una descrizione dettagliata dell'interfaccia Modalità Avanzata di BitDefender. Vi spieghiamo come configurare ed utilizzare tutti i moduli di BitDefender in modo da proteggere efficacemente il vostro computer da ogni tipo di minaccia malware (virus, spyware, rootkit ed altro).

Integrazione in Software Windows e di terzi . Mostra come utilizzare le opzioni di BitDefender dal menu contestuale di Windows e dalla barra degli strumenti BitDefender integrata in programmi supportati di terze parti.

Come fare. Procedura per le funzioni più comuni in BitDefender

Risoluzione dei problemi e aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà. E' inclusa anche una sezione FAQ (Domande frequenti).

CD di soccorso BitDefender. Descrizione del CD di soccorso BitDefender. Consente di comprendere e utilizzare le funzioni offerte da questo CD di avvio.

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverai tra le pagine di questo documento.

3. Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutta l'informazione con la nostra massima capacità, ma potresti trovare che le caratteristiche siano cambiate (o persino che abbiamo commesso degli errori). Per favore scrivi per parlarci su qualsiasi errore trovi in questo libro o come credi che possa essere migliorato, per aiutarci a fornirti la migliore documentazione possibile.

Facci sapere inviando una e-mail a documentation@bitdefender.com.

Importante
Per una comunicazione efficiente, vi invitiamo a scrivere i vostri documenti e le e-mails in lingua Inglese.

Installazione e rimozione

1. Requisiti del sistema

È possibile installare BitDefender Antivirus 2010 solo su computer con i seguenti sistemi operativi:

- Windows XP (32/64 bit) con Service Pack 2 o superiore
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1 o successivo
- Windows 7 (32/64 bit)

Prima dell'installazione, assicurarsi che il computer soddisfa i prerequisiti hardware e software minimi.

Nota
Per verificare il sistema operativo sul computer e l'informazione hardware, fare clic con il pulsante destro del mouse su **Risorse del computer** sul desktop e quindi selezionare **Proprietà** dal menu.

1.1. Requisiti minimi di sistema

- 450 MB di spazio disponibile su disco rigido
- Processore da 800 MHz
- RAM:
  - 512 MB per Windows XP
  - 1 GB per Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.2. Requisiti di sistema consigliati

- 600 MB di spazio disponibile su disco rigido
- Intel CORE Duo (1.66 GHz) o processore equivalente
- RAM:
  - 1 GB per Windows Vista/Windows 7
  - 1,5 GB per Windows Vista
- Internet Explorer 7 (o superiore)
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.3. Software supportato

La protezione antiphishing viene fornita solo per:

- Internet Explorer 6.0 o superiore
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

La criptazione del Chat (IM) viene fornita solo per:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Preparazione all'Installazione

Prima di installare BitDefender Antivirus 2010, completare questi passi preliminari per assicurarsi che l'installazione funzioni senza problemi:

- Assicurarsi che il computer su cui si desidera installare BitDefender risponda ai requisiti minimi di sistema. Se il computer non risponde ai requisiti minimi di sistema, BitDefender non verrà installato o se installato non funzionerà correttamente e causerà rallentamenti e instabilità del sistema. Per un elenco completo dei requisiti di sistema, fare riferimento a *«Requisiti del sistema»* (p. 2).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovere qualsiasi altro software di sicurezza dal computer. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Windows Defender sarà disabilitato per default prima dell'avvio dell'installazione.

3. Installazione di BitDefender

E' possibile installare BitDefender dal CD di installazione BitDefender oppure utilizzando il file di installazione scaricato sul computer dal sito di BitDefender o da altri siti web autorizzati (ad esempio il sito web di un partner di BitDefender o un negozio on-line) Il file di installazione può essere scaricato dal sito web di BitDefender al seguente indirizzo: http://www.bitdefender.it/site/Downloads/.

- Per installare BitDefender da CD, inserire il CD nel lettore. Dopo alcuni istanti verrà visualizzata una finestra di benvenuto. Seguire le istruzioni per avviare l'installazione.

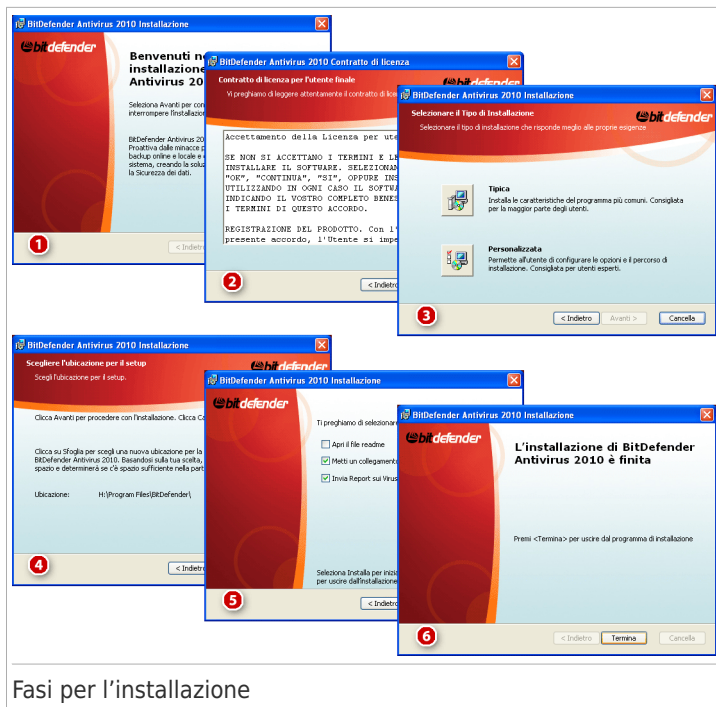
Nota

La schermata di benvenuto prevede l'opzione di copiare il pacchetto di installazione dal CD ad un dispositivo USB. Questo è utile se necessiti di installare BitDefender su di un PC che non possiede un drive CD (ad esempio un netbook). Inserisci il dispositivo USB nel drive USB e clicca **Copia su USB**. In seguito, spostati sul PC senza drive CD, inserisci il dispositivo USB nel drive USB e fai doppio click su `runsetup.exe` dalla cartella nella quale hai salvato il pacchetto di installazione.

Se non appare la schermata di benvenuto, seguire questo percorso `Products\Antivirus\install\it\` dalla directory iniziale del CD e fare doppio clic su `runsetup.exe`.

- Per installare BitDefender utilizzando il file di installazione scaricato sul computer, individuare il file e fare doppio clic su di esso.

Il programma di installazione controllerà innanzitutto il sistema per convalidare l'installazione. Se l'installazione viene convalidata, apparirà l'assistente di setup. L'immagine seguente illustra i passaggi dell'assistente di setup.

Fasi per l'installazione

Seguire questi passi per installare Antivirus BitDefender 2010:

1. Selezionare **Avanti**. E' possibile annullare l'installazione in qualsiasi momento facendo clic su **Annulla**.

   BitDefender Antivirus 2010 avvisa se vi sono altri prodotti antivirus installati sul computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.

   Avvertimento

   Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

2. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto**

   Importante

   Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. Il processo di installazione verrà abbandonato ed uscirete dal setup.

3. Selezionare il tipo di installazione da eseguire.
   - **Tipica** - per installare il programma immediatamente, utilizzando le opzioni di installazione di default. Se si seleziona questa opzione, passare al Passo 6.
   - **Personalizzata** - per configurare le opzioni di installazione e quindi installare il programma. Questa opzione permette di modificare il percorso di installazione.
4. Per default, Antivirus BitDefender 2010 verrà installato in `C:\Program Files\BitDefender\BitDefender 2010`. Se si desidera modificare il percorso d'installazione, fare clic su **Sfoglia**, quindi selezionare, la cartella dove si desidera installare Antivirus BitDefender 2010.

   Selezionare **Avanti**.
5. Selezionare le opzioni relative al processo di installazione. Le opzioni consigliate sono selezionate per default:
   - **Apri il file readme** - per aprire il file leggimi al termine dell'installazione.
   - **Metti un collegamento sul desktop** - per mettere un collegamento a BitDefender Antivirus 2010 sul desktop al termine dell'installazione.
   - **Disabilita Caching DNS** - per disabilitare il Caching DNS (Domain Name System). Il servizio Client DNS può essere utilizzato da applicazioni malevole per inviare informazioni attraverso la rete senza il consenso dell'utente.
   - **Invia Rapporti Virus** - per inviare rapporti sulla scansione antivirus al Laboratorio BitDefender per l'analisi. I report non conterranno dati confidenziali, come il vostro nome o indirizzo IP, e non verranno utilizzati per scopi commerciali.
   - **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

   Fare clic su **Installa** per avviare l'installazione. Se non è stato ancora installato, BitDefender installerà per prima .NET Framework 1.1.
6. Attendere che l'installazione sia completata e fare clic su **Termina**. Vi verrà richiesto di riavviare il sistema in modo che l'assistente di setup completi il processo di installazione. Si raccomanda di farlo al più presto.

Importante

Una volta completata l'installazione e riavviato il computer, compariranno un assistente di registrazione ed un assistente di configurazione. Completare queste procedure guidate per registrare e configurare BitDefender Antivirus 2010 e per creare un account BitDefender.

Se sono state accettate le impostazioni di default per il percorso di installazione, è possibile vedere una nuova cartella chiamata `BitDefender` in `Program Files` che contiene la sotto-cartella `BitDefender 2010`.

3.1. Procedura guidata di Registrazione

La prima volta che avviarete il computer dopo l'installazione, comparirà l'assistente per la registrazione. L'assistente vi aiuterà a registrare BitDefender ed a configurare un conto BitDefender.

Devi creare un account per poter ricevere gli update di BitDefender. L'account BitDefender ti da accesso al supporto tecnico gratis, a offerte speciali e promozioni. Se avete perso la vostra chiave di licenza BitDefender, potete logarvi sul vostro conto in http://myaccount.bitdefender.com per recuperarla.

Nota

Se non si desidera seguire questo assitente, fare click su **Annulla**. Potete aprire la registrazione guidata in qualsiasi momento facendo click sul link **Registrazione**, situato in fondo all'interfaccia del utente.

3.1.1. Passo 1 - Registrare BitDefender Antivirus 2010

Registrazione

BitDefender Antivirus 2010 ha un periodo di prova di 30 giorni. Per continuare a valutare il prodotto, selezionare **Voglio continuare a valutare BitDefender** e fare clic su **Avanti**.

Per registrare BitDefender Antivirus 2010:

1. Selezionare **Voglio registrare BitDefender con una nuova chiave di licenza**.

2. Inserire la chiave di licenza nel campo di modifica.

Nota

Potete trovare la vostra chiave di licenza:

- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

3. Fare clic su **Registra Ora**.
4. Selezionare **Avanti**.

Se viene rilevata una chiave di licenza BitDefender valida sul sistema, è possibile continuare ad usare tale chiave facendo clic su **Avanti**.

3.1.2. Passo 2 - Creare un Account BitDefender

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 10)
- «Ho già un account BitDefender» (p. 10)

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.
   - **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
   - **Confermare Password** - inserire di nuovo la password specificata previamente.

   Nota

   Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.
3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Nota
Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

3.2. Procedura guidata di Configurazione

Una volta completata la registrazione, comparirà l'assistente per la configurazione. Questo assistente permette di configurare le impostazioni principali e l'interfaccia utente di BitDefender in modo che rispondano al meglio alle vostre esigenze. Al termine dell'assistente sarà possibile aggiornare i file del prodotto e le firme dei malware ed effettuare una scansione dei file di sistema e delle applicazioni per assicurarsi che non siano infetti.

L'assistente è costituto da alcuni semplici passaggi. Il numero di passaggi dipende dalle scelte effettuate. Tutti i passaggi vengono presentati qui, ma si verrà avvisati quando le proprie scelte ne influenzano il numero.

Il completamento dell'assistente non è obbligatorio; in ogni caso si consiglia di farlo per risparmiare tempo e assicurarsi che il sistema sia sicuro ancor prima dell'installazione di BitDefender Antivirus 2010. Se non si desidera seguire questo assitente, fare click su **Annulla**. BitDefender vi informerà sui componenti che dovrete configurare all'apertura del interfaccia del utente.

3.2.1. Passo 1 - Selezione del Profilo di Utilizzo

Profili di Utilizzo

Fare clic sul pulsante che descrive al meglio le attività compiute sul computer (il profilo di utilizzo).

Opzione	Descrizione
Tipico	Fare clic qui se il PC è utilizzato principalmente per navigare e per attività multimediali.
Giocatore	Fare clic qui se il PC è utilizzato principalmente per giocare.
Personalizzato	Fare clic qui se si desiderano configurare tutte le impostazioni principali di BitDefender.

Il profilo di utilizzo può essere reimpostato in un secondo momento dall'interfaccia del prodotto.

3.2.2. Passo 2 - Descrivere il Computer

Descrizione del Computer

Selezionare le opzioni che si applicano al computer:

- **Questo computer si trova in una rete domestica.** Selezionare questa opzione se si desidera gestire il prodotto BitDefender installato sul computer da remoto (da un altro computer). Un ulteriore passaggio dell'assistente permetterà la configurazione del modulo di Gestione della Rete Domestica.
- **Questo computer è un notebook.** Selezionare questa opzione se si desidera che la Modalità Laptop sia abilitata per default. Nella Modalità portatile, le attività di scansione programmate non vengono eseguite, poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

Selezionare **Successivo** per continuare.

3.2.3. Passo 3 - Selezionare l'Interfaccia Utente

Modalità di visualizzazione dell'interfaccia dell'utente.

Fare clic sul pulsante che meglio descrive le capacità informatiche dell'utente per selezionare una modalità di visualizzazione dell'interfaccia utente appropriata. È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di BitDefender.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto.

Modalità	Descrizione
	È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

3.2.4. Passo 4 - Configurare la Rete BitDefender

Nota
Questo passaggio appare solo se si è specificato che il computer è collegato ad una rete domestica al Passaggio 2.

Configurazione della Rete BitDefender

BitDefender vi permette di creare una rete virtuale con i computer della vostra famiglia e di gestire i prodotti BitDefender installati su questa rete.

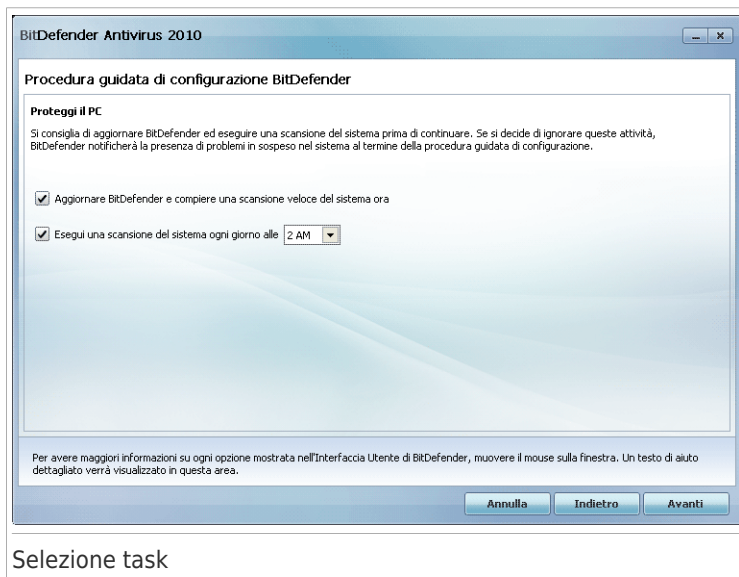
Se vuoi che questo computer faccia parte della Rete Domestica BitDefender, segui questi passi:

1. Selezionare **Abilita Rete Domestica**.

2. Inserire la stessa password di amministratore in ogni campo di modifica. La password permette ad un amministratore di gestire questo prodotto BitDefender da un altro computer.

Selezionare **Successivo** per continuare.

3.2.5. Passo 5 - Selezionare le Attività da eseguire

Selezione task

Impostare BitDefender per l'esecuzione di attività importanti per la sicurezza del sistema. Sono disponibili le seguenti opzioni:

- **Aggiorna BitDefender ed esegui una scansione veloce del sistema ora** - al passaggio successivo le firme dei virus e i file di prodotto di BitDefender verranno aggiornati per proteggere il computer contro le minacce più recenti. Inoltre, immediatamente al termine dell'aggiornamento, BitDefender effettuerà una scansione dei file nelle cartelle `Windows` e `Programmi` per assicurarsi che non siano infetti. Queste cartelle contengono file del sistema operativo e delle applicazioni installate e sono di norma le prime ad essere infettate.
- **Esegui una scansione del sistema ogni giorno alle 2** - imposta BitDefender in modo da eseguire una scansione standard del computer ogni giorno alle 2. Per modificare l'orario di esecuzione della scansione, fare clic sul menu e selezionare l'orario di inizio desiderato. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

Nota

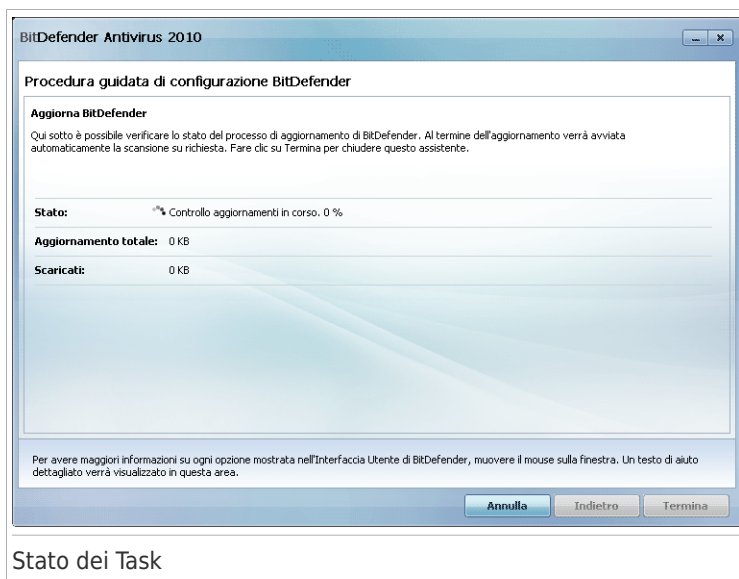
Se in un secondo momento si desidera modificare l'orario di programmazione della scansione, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**.
4. Fare clic con il tasto destro sull'attività **Scansione del Sistema** e selezionare **Programma**. Apparirà una nuova finestra.
5. Cambia la frequenza e l'ora di avvio se necessario
6. Selezionare **Applica** per salvare le modifiche.

Vi raccomandiamo di abilitare queste opzioni prima di passare al passo successivo per assicurare la sicurezza del vostro sistema. Selezionare **Successivo** per continuare.

Se viene deselezionata la prima casella di controllo, non vi sono attività da eseguire nell'ultimo passaggio dell'assistente. Fare clic su **Termina** per completare l'assistente.

3.2.6. Passo 6 - Fine

Stato dei Task

Attendere che BitDefender aggiorni le firme del malware e i motori di scansione. Non appena l'aggiornamento è completato, verrà avviata una scansione rapida del sistema. La scansione avverrà in modo silenzioso, in background. E' possibile seguire

l'icona di avanzamento della scansione nell'area di notifica. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Fare clic su **Termina** per completare l'assistente. Non devi attendere il termine della scansione

Nota

La scansione impiegherà alcuni minuti. Quando è terminata, aprire la finestra di scansione per controllare i risultati e assicurarsi che il sistema sia pulito. Se un virus è rilevato durante una scansione, dovresti aprire immediatamente BitDefender ed avviare una scansione completa

4. Upgrade

E' possibile effettuare l'aggiornamento a BitDefender Antivirus 2010 se si sta utilizzando BitDefender Antivirus 2010 beta oppure le versioni 2008 o 2009.

Vi sono due modi per eseguire l'aggiornamento:

- Installare BitDefender Antivirus 2010 direttamente su una versione precedente. Se installi direttamente sopra la versione 2009, la Quarantena viene importata automaticamente.
- Rimuovere la versione precedente, quindi riavviare il computer e installare la nuova versione come descritto al capitolo «*Installazione di BitDefender*» (p. 5). Non verrà salvata alcuna impostazione del prodotto. Utilizzare questo metodo di aggiornamento se l'altro metodo non ha avuto successo.

5. Riparare o Rimuovere BitDefender

Se si desidera riparare o rimuovere BitDefender Antivirus 2010, seguire questo percorso dal menu di avvio di Windows: **Start** → **Programmi** → **BitDefender 2010** → **Ripara o Rimuovi**.

Vi verrà richiesto di confermare la vostra scelta selezionando **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Riparare** - per re-installare tutte le componenti del programma installate dal setup precedente.

  Scegliendo di riparare BitDefender, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

  Riavviare il computer quando venga richiesto, e quindi selezionare **Installare** per reinstallare Antivirus BitDefender 2010.

  Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

- **Rimuovi** - per rimuovere tutte le componenti installate.

Nota
Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

Scegliendo di rimuovere BitDefender, apparirà una nuova finestra.

Importante

Solo Windows Vista! Rimuovendo BitDefender, non sarete più protetti contro le minacce malware come virus e spyware. Se desiderate che Windows Defender venga attivato dopo aver disinstallato BitDefender, selezionare la casella di controllo corrispondente.

Selezionare**Rimuovere** per iniziare la rimozione di Antivirus BitDefender 2010 dal computer.

Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.

Nota
Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `BitDefender` dei `Program Files`.

Iniziando

6. Panoramica

Una volta che avrete installato BitDefender il vostro computer sarà protetto. Se non hai completato la procedura di assistenza, devi aprire BitDefender e correggere eventuali errori. Devi configurare i componenti di BitDefender o prendere azioni preventive per proteggere i tuoi computer e i tuoi dati Se lo desideri, puoi fare in modo che Bitdefender non ti allerti per determinati problemi.

Se non hai registrato il prodotto (e/o non hai creato un account BitDefender) ricorda di farlo prima che il periodo di prova finisca. E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato. Per ulteriori informazioni sulla registrazione, ti preghiamo di riferirti a *«Registrazione e Il mio Account»* (p. 48).

6.1. Apertura di BitDefender in corso

Per accedere all'interfaccia principale di BitDefender Antivirus 2010, usare il menu Avvio di Windows, seguendo il percorso: **Start** → **Tutti i programmi** → **BitDefender 2010** → **BitDefender Antivirus 2010** o più rapidamente facendo doppio clic sull'icona BitDefender presente nella barra delle applicazioni.

6.2. Modalità di visualizzazione dell'interfaccia dell'utente.

BitDefender Antivirus 2010 soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di BitDefender.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.

Modalità	Descrizione
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

La modalità interfaccia utente viene selezionata nella procedura guidata di configurazione. Questa procedura guidata appare dopo la procedura guidata di registrazione, la prima volta che si accede al computer dopo aver installato il prodotto. Se annulli la procedura guidata di registrazione o quella di configurazione, la modalità di interfaccia utente sarà la Modalità Intermedia per default.

Per cambiare modalità di interfaccia utente, eseguire i seguenti passi:

1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.2.1. Modalità inesperto

Se si è inesperti in materia di computer, l'interfaccia Modalità inesperto potrebbe essere la scelta migliore. Questa modalità è semplice da utilizzare e richiede pochissimo intervento da parte dell'utente.

Modalità inesperto

La finestra è suddivisa in quattro sezioni principali:

- **Stato della sicurezza** informa in merito ai problemi che riguardano la sicurezza del computer e aiuta a risolverli. Facendo clic su **Risolvi tutti i problemi**, una procedura guidata aiuterà a risolvere facilmente minacce alla sicurezza del computer e dei dati. Per ulteriori informazioni, far riferimento a *«Risolvi i Problemi»* (p. 37).

- In **Proteggi il PC** è possibile trovare le attività che proteggono il computer e i dati. Le attività disponibili che possono essere eseguite sono diverse a seconda del profilo di utilizzo selezionato.

  - Il pulsante **Esegui scansione Ora** avvia una scansione standard del sistema alla ricerca di virus, spyware e altro malware. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

  - Il pulsante **Aggiorna Ora** permette di aggiornare le firme dei virus e i file di prodotto di BitDefender. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento. Se vengono rilevati degli aggiornamenti, questi vengono automaticamente scaricati ed installati sul computer.

  - Quando viene selezionato il profilo **Tipico** il pulsante **Controllo Vulnerabilità** esegue un assistente che permette di trovare e risolvere le vulnerabilità del sistema, quali ad esempio del software obsoleto o degli aggiornamenti di

Windows mancanti. Per ulteriori informazioni fare riferimento alla sezione *«Procedura guidata di Controllo delle vulnerabilità»* (p. 65).

- Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.

- In **Manutenzione del PC** è possibile trovare le attività aggiuntive che proteggono il computer e i dati.
  - **Scansione Approfondita del Sistema** avvia una scansione completa del sistema alla ricerca di tutti i tipi di malware.
  - **Scansione Documenti** effettua la scansione alla ricerca di virus e altro malware nelle cartelle utilizzate più comunemente: `Documenti` e `Desktop`. Questo assicura la sicurezza dei documenti, un'area di lavoro sicura e l'esecuzione di applicazioni pulite all'avvio.
  - **Scansione Esecuzione Automatica** effettua la scansione degli elementi che vengono automaticamente eseguiti quando si effettua l'accesso a Windows.
- **Profili D'uso** indica il profilo di utilizzo correntemente selezionato. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

  Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni fondamentali»* (p. 41).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto BitDefender Antivirus 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.

Link	Descrizione
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.2.2. Modalità intermedia

Ricolta agli utenti con una conoscenza media dei computer, la Modalità Intermedia è una interfaccia semplice che fornisce accesso a tutti i moduli di base. Si dovranno monitorare avvertimenti e avvisi critici e risolvere problemi.

Modalità intermedia

La finestra Modalità Intermedia contiene 5 schede. La seguente tabella descrive brevemente ogni scheda. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 72) di questo manuale.

Tab	Descrizione
Dashboard	Visualizza lo stato di sicurezza del sistema e permette di ripristinare il profilo di utilizzo.
Antivirus	Mostra lo stato del modulo antivirus, il quale vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus.

Tab	Descrizione
Antiphishing	Mostra lo stato dei moduli che ti proteggono contro il phishing (furto di informazioni personali) mntre sei online
Vulnerabilità	Mostra lo stato del modulo vulnerabilità e vi aiuta a mantenere sempre aggiornato il software cruciale per il vostro computer. Qui puoi correggere facilmente ogni vulnerabilità che può avere il tuo PC
Rete	Mostra la struttura della rete domestica BitDefender. Qui puoi attivare varie azioni per configurare e cgestire i prodotti BitDefender installati sulla tua rete casalinga In questo modo puoi gestire la sicurezza della tua rete di casa da una singola postazione

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni fondamentali»* (p. 41).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

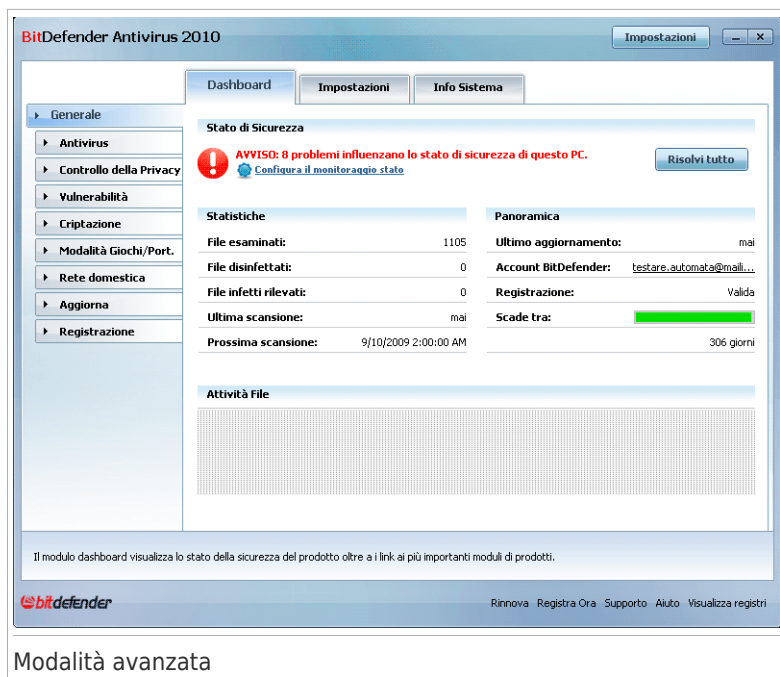
Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto BitDefender Antivirus 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.2.3. Modalità avanzata

La Modalità Avanzata dà accesso ad ogni specifico componente di BitDefender. Qui è possibile configurare in dettaglio BitDefender.

Nota

La Modalità Avanzata è adatta per utenti dotati di conoscenze informatiche superiori alla media, che conoscono a quali tipi di pericoli è esposto un computer e come funzionano i programmi di sicurezza.

Modalità avanzata

Sulla parte sinistra della finestra c'è un menu contenente tutti i moduli di sicurezza. Ogni modulo consiste di una o più schede che permettono la configurazione delle impostazioni di sicurezza corrispondenti oppure permettono di eseguire attività di amministrazione e di sicurezza. La seguente tabella descrive brevemente ogni modulo. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 94) di questo manuale.

Modulo	Descrizione
Generale	Vi permette di accedere alle impostazioni generali o di visualizzare la dashboard e le informazioni dettagliate di sistema.
Antivirus	Vi permette di configurare in dettaglio il vostro scudo antivirus e le operazioni di scansione, impostare le eccezioni e configurare il modulo di quarantena.
Controllo Privacy	Vi permette di prevenire il furto di dati dal vostro computer e proteggere la vostra privacy mentre siete online.

Modulo	Descrizione
Vulnerabilità	Vi permette di mantenere aggiornato il software cruciale del vostro computer.
Criptazione	Vi permette di criptare le comunicazioni su Yahoo e Windows Live (MSN).
Modalita' Gioco/Portatile	Vi permette di posporre i task programmati di BitDefender mentre il vostro portatile funziona con le batterie ed anche di eliminare allarmi e pop-up mentre giocate.
Rete	Vi permette di configurare e gestire diversi computer nella vostra famiglia.
Aggiornamento	Vi permette di ottenere informazioni sugli ultimi aggiornamenti, di aggiornare il prodotto e di configurare in dettaglio il processo di aggiornamento.
Registrazione	Permette di registrare BitDefender Antivirus 2010, di cambiare la chiave di licenza o di creare un account BitDefender.

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni fondamentali»* (p. 41).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto BitDefender Antivirus 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.3. Icona barra delle applicazioni

Per gestire tutto il prodotto più velocemente, è possibile utilizzare l'icona BitDefender nella barra delle applicazioni. Se si fa doppio clic su questa icona, BitDefender si

aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto BitDefender.

Icona della barra delle applicazioni

- **Mostra** - apre l'interfaccia di BitDefender.
- **Help** - apre il file di aiuto, che spiega nel dettaglio come configurare e usare BitDefender Antivirus 2010.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.
- **Risolvi tutti i problemi** - aiuta a rimuovere tutte le vulnerabilità di sicurezza correnti. Se l'opzione non è disponibile, non ci sono errori da riolvere. Per ulteriori informazioni, far riferimento a *«Risolvi i Problemi»* (p. 37).
- **Modalità Gioco SI/NO** - attiva / disattiva la Modalità Gioco.
- **Aggiorna adesso** - inizia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.
- **Impostazioni di base** - apre una finestra dove è possibile cambiare la modalità interfaccia utente e abilitare e disabilitare il prodotto principale. Per ulteriori informazioni, far riferimento a *«Configurazione delle Impostazioni fondamentali»* (p. 41).

L'icona BitDefender nell'area di notifica fornisce informazioni relative ai problemi del computer o al funzionamento del prodotto, visualizzando un simbolo speciale come segue:

Triangolo rosso con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.
Lettera G: Il prodotto funziona inGame Mode.

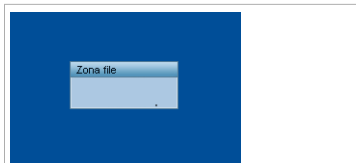
Se BitDefender non è in funzione, l'icona nell'area di notifica è disattivata. Questo si verifica normalmente quando la licenza è scaduta. Può anche verificarsi quando i servizi di BitDefender non rispondono o quando altri errori interferiscono con il normale funzionamento di BitDefender.

6.4. Barra di Attività della Scansione

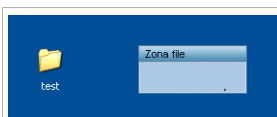
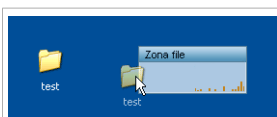
La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

Le barre grigie (**Zona File**) indicano il numero di file esaminati al secondo, in una scala da 0 a 50.

Nota

La Barra delle attività di scansione vi informerà quando la protezione in tempo reale sia disattivata mostrando una croce rossa sulla **Zona File**.

Barra di Attività della Scansione

6.4.1. Scansiona File e Cartelle

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file

Abbandonare il file

Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

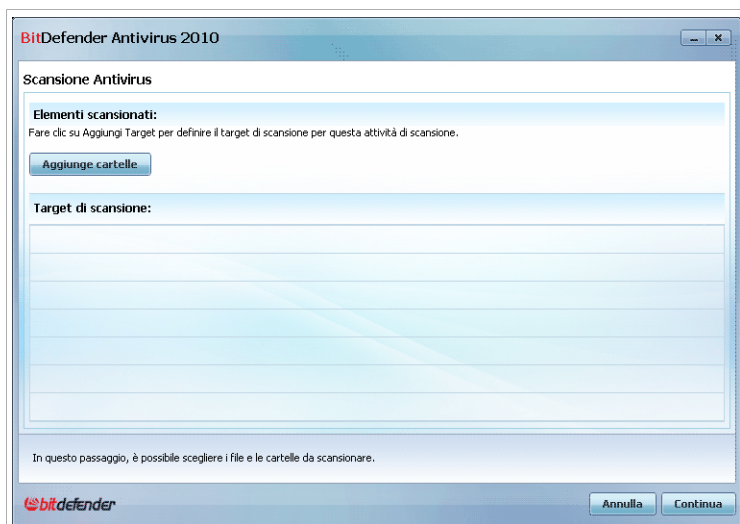
6.4.2. Disabilita/ripristina la barra di attività scansione

Quando non si vuole più vedere la visualizzazione grafica, si deve semplicemente premere sulla stessa con il pulsante destro e selezionare **Nascondi**. Per ripristinare la barra delle attività di scansione, seguire questi passi:

1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Barra Attività di Scansione**.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.5. Scansione Manuale di BitDefender

La scansione Manuale BitDefender consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando BitDefender Manual Scan.

Per accedere alla Scansione Manuale BitDefender utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio** → **Programmi** → **BitDefender 2010** → **Scansione Manuale di BitDefender** Apparirà la finestra seguente:

Scansione Manuale di BitDefender

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usato principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

6.6. Modalità giochi e Modalità portatile

Alcune attività del computer, ad esempio giochi o presentazioni, richiedo una maggiore risposta e performance, dal sistema e nessuna interruzione. Quando il laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

Per adattarsi a queste situazioni particolari, BitDefender Antivirus 2010 include due modalità operative speciali:

- Modalità giochi
- Modalità portatile

6.6.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Minimizzare il consumo di memoria e di tempo del processore.
- Posporre scansioni ed aggiornamenti automatici.
- Eliminare tutti gli allarmi ed i pop-up.
- Eseguire la scansione solo dei file più importanti.

Mentre siete in Modalità Gioco, potete vedere la lettera G sull'icona BitDefender.

Uso della Modalità Gioco.

Di default, BitDefender entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista BitDefender dei giochi conosciuti o quando un'applicazione passa a schermo pieno. BitDefender tornerà automaticamente alla modalità normale quando si chiude il gioco o quando l'applicazione rilevata esce dallo schermo intero.

Se si vuole attivare manualmente la Modalità giochi, utilizzare uno dei metodi seguenti:

- fare clic con il pulsante destro sull’icona di BitDefender nella barra di sistema e selezionare **Attivare Modalità giochi**.
- Premere `Ctrl+Shift+Alt+G` (la hotkey di default).

Importante
Non dimenticare di disattivare la Modalità Gioco quando avete finito. Per farlo, utilizzare gli stessi metodi usati per attivarla.

Modifica Hotkey della Modalità Gioco.

Per modificare la hotkey, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Modalità giochi / portatile** nel menu a sinistra.
3. Fare clic sulla scheda **Modalità giochi**.
4. Fare clic sul pulsante **Impostazioni Avanzate**.
5. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:

- Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
- Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

Nota
Togliere lo spunto da **Usare HotKey** disabiliterà la hotkey.

6. Selezionare **Applica** per salvare le modifiche.

6.6.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di BitDefender sul consumo di energia mentre questi apparecchi funzionino con la batteria. Nella Modalità portatile, le attività di scansione programmate non vengono eseguite, poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

BitDefender rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, BitDefender uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per utilizzare la Modalità portatile, è necessario specificare nella procedura guidata di configurazione che si sta utilizzando un laptop. Se non si è selezionata l'opzione appropriata quando si eseguiva la procedura guidata, è possibile abilitare la Modalità portatile successivamente nel seguente modo:

1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Individuazione Modalità portatile**.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.7. Rilevamento dispositivo automatico

BitDefender rileva automaticamente quando si collega un dispositivo rimovibile al computer e chiede di eseguirne la scansione prima che si acceda ai suoi file. Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD

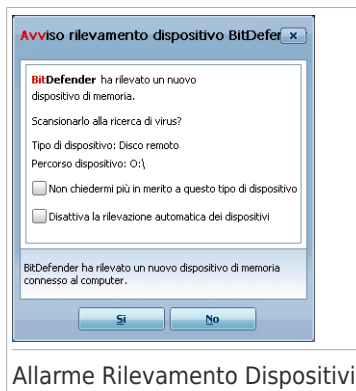
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- unità di rete (remote) mappate

Quando un tale dispositivo viene rilevato, viene visualizzata una finestra di avviso.

Per scansionare il dispositivo di archiviazione, è sufficiente fare clic su **Sì**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

Allarme Rilevamento Dispositivi

Se non si desidera scansionare il dispositivo, si deve fare clic su **No**. In questo caso, si possono ritenere utili una di queste opzioni:

- **Non farmi più domande su questo tipo di dispositivo** - BitDefender non chiederà più di eseguire la scansione di dispositivi di questo tipo quando sono collegati al tuo computer.
- **Disabilita rilevamento automatico dispositivi** - Non verrà più chiesto di eseguire la scansione di nuovi dispositivi di archiviazione quando sono collegati al computer.

Se per sbaglio si disabilita il rilevamento automatico dei dispositivi di archiviazione e si desidera abilitarlo, o se si desidera configurarne le impostazioni, eseguire questi passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antivirus>Virus Scan**.
3. Nell'elenco delle attività di scansione, individuare l'attività **Scansione rilevamento dispositivi**.
4. Fare clic sull'attività e selezionare **Apri**. Apparirà una nuova finestra.
5. Sulla scheda **Panoramica**, configurare le opzioni di scansione come necessarie. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Configurazione delle Impostazioni di Scansione»* (p. 119).
6. Sulla scheda **Rilevamento**, scegliere i tipi di dispositivi di archiviazione da rilevare.
7. Fare clic su**OK** per salvare e applicare i cambiamenti.

7. Risolvi i Problemi

BitDefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer e dei dati. Per default il sistema controlla solo una serie di problemi considerati molto importanti. Tuttavia è possibile configurare il sistema come si desidera, scegliendo di quali problemi specifici si desidera ricevere una notifica.

I problemi in sospeso vengono notificati nel modo seguente:

- Viene visualizzato un simbolo speciale sull'icona BitDefender nell'area di notifica ad indicare la presenza di problemi in sospeso.

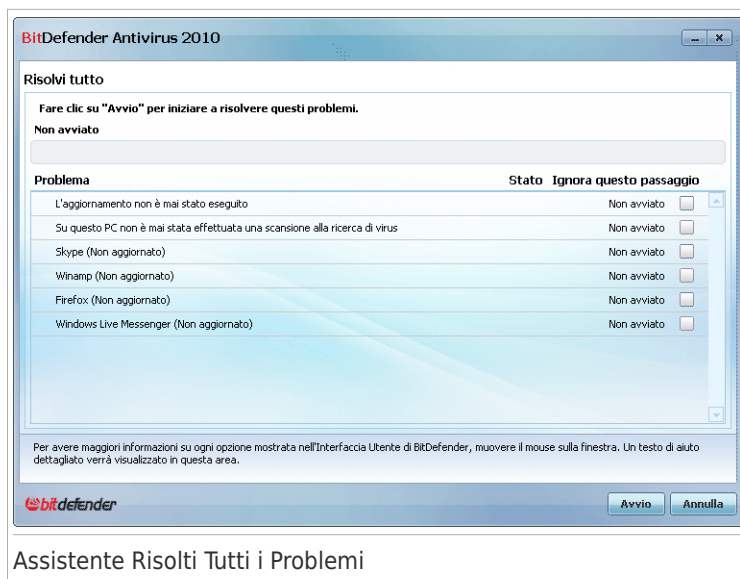
  Triangolo rosso con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

  Inoltre muovendo il cursore sull'icona un pop-up confermerà l'esistenza di problemi in sospeso.

- Quando viene aperto BitDefender, l'area Stato della Sicurezza indicherà il numero di problemi del sistema.
  - In Modalità Intermedia, lo stato della sicurezza viene visualizzato nella scheda **Dashboard**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** per controllare lo stato della sicurezza.

7.1. Assistente Risolti Tutti i Problemi

Il modo più semplice di risolvere i problemi esistenti è di seguire le istruzioni passo-passo dell'assistente **Risolvi Tutti i Problemi**. L'assistente aiuta a rimuovere con facilità qualsiasi minaccia per la sicurezza del computer e dei dati. Per aprire l'assistente, compiere una delle seguenti operazioni:

- Fare clic on il pulsante di destra sull icona BitDefender nell'area di notifica e selezionare **Risolvi Tutti i Problemi**.
- Apri BitDefender. A seconda della modalità dell'interfaccia utente, procedere come segue:
  - In Modalità Inesperto, fare clic su **Risolvi Tutti i Problemi**.
  - In Modalità Intermedia, andare alla scheda **Dashboard** e fare clic su **Risolvi Tutti i Problemi**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** e fare clic su **Risolvi Tutti i Problemi**.

Assistente Risolti Tutti i Problemi

L'assistente visualizza l'elenco delle vulnerabilità di sicurezza esistenti sul computer.

Tutti i problemi attuali sono stati selezionati per essere risolti. Se vi è un problema che non si desidera risolvere, selezionare la casella di controllo corrispondente. In questo modo lo stato cambierà su **Ignora**.

Nota

Se non si desidera ricevere notifiche relative a particolari problemi è necessario configurare di conseguenza il sistema di controllo, come descritto alla sezione successiva.

Per risolvere i problemi selezionati, fare clic su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che l'assistente permette di risolvere possono essere raggruppati nelle seguenti categorie principali:

- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che è necessario eseguire.** Un esempio di tali attività è la scansione del computer. Si consiglia di eseguire la scansione del compuer almeno una volta alla settimana. BitDefender compirà questa attività automaticamente nella maggior parte dei casi. Tuttavia se il programma di

scansione è stato modificato o non è stato completato, si riceverà un avviso relativo a questo problema.

Nel risolvere tali problemi, un assistente permette di completare con successo l'attività.

- **Vulnerabilità del sistema.** BitDefender controlla automaticamente il sistema alla ricerca di vulnerabilità e fornisce avvisi al riguardo. Le vulnerabilità di sistema includono quanto segue:
  - password deboli per gli account utente di Windows.
  - software obsoleto sul computer.
  - aggiornamenti di Windows mancanti.
  - Gli Aggiornamenti Automatici di Windows sono disabilitati.

  Quando è necessario risolvere tali problemi, viene avviato l'assistente scansione vulnerabilità. Questo assistente permette di risolvere le vulnerabilità di sistema rilevate. Per ulteriori informazioni fare riferimento alla sezione *«Procedura guidata di Controllo delle vulnerabilità»* (p. 65).

7.2. Configurazione del monitoraggio problemi

Il sistema di controllo dei problemi è preconfigurato per il monitoraggio e l'avviso relativo ai più importanti problemi che possono influenzare la sicurezza del computer e dei dati. Ulteriori problemi possono essere monitorati in base alle scelte compiute nell'assistente di configurazione (quando viene configurato il profilo di utilizzo). Oltre ai problemi monitorati per default, vi sono molti altri problemi su cui si può essere informati.

E' possibile configurare il sistema di controllo per rispondere al meglio alle proprie esigenze di sicurezza, selezionando di quali problemi specifici si desidera essere informati. Questa operazione è possibile in Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio può essere configurato da posizioni separate. Attenersi alla seguente procedura:
  1. Andare alle schede **Antivirus**, **Antiphishing** oppure **Vulnerabilità**.
  2. Fare clic su **Configura stato monitoraggio**.
  3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

  Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 72) di questo manuale.

- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura stato monitoraggio**.

3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 95).

8. Configurazione delle Impostazioni fondamentali

È possibile configurare le impostazioni principali del prodotto (inclusa la modifica la modalità di visualizzazione dell'interfaccia utente) dalla finestra delle impostazioni fondamentali. Per aprirla, seguire una delle seguenti procedure:

- Aprire BitDefender e fare clic sul pulsante **Impostazioni** in alto a destra.
- Fare clic con i pulsante di destra sulla icona BitDefender nella barra delel applicazioni e selezionare **Impostazioni fondamentali**.

Nota

Per configurare in dettaglio le impostazioni del prodotto, utilizzare l'interfaccia nella Modalità Avanzata. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 94) di questo manuale.

Impostazioni di base

Le impostazioni sono suddivise in tre categorie:

- Impostazioni interfaccia utente
- Impostazioni sulla sicurezza
- Impostazioni generali

Per applicare e salvare le modifiche apportate alla configurazione, fare clic su **OK**. Per chiudere la finestra senza salvare i cambiamenti, fare clic su **Elimina**.

8.1. Impostazioni interfaccia utente

In quest'area è possibile commutare la modalità di visualizzazione dell'interfaccia utente e ripristinare il profilo di utilizzo.

Commutazione della modalità di visualizzazione dell'interfaccia utente. Come descritto nella sezione *«Modalità di visualizzazione dell'interfaccia dell'utente.»* (p. 22), ci sono tre modalità di visualizzazione dell'interfaccia utente. Ogni modalità di visualizzazione dell'interfaccia utente è progettata per una categoria specifica di utenti, in base alla loro conoscenza dei computer. In questo modo, l'interfaccia utente può soddisfare i requisiti di tutti i tipi di utenti, dai principianti agli esperti.

Il primo pulsante mostra la modalità di visualizzazione dell'interfaccia utente attuale. Per cambiare la modalità interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità Avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

Reimpostazione del profilo di utilizzo. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

Per riconfigurare il profilo di utilizzo, fare clic su **Reimposta Profilo di Utilizzo** e seguire l'assistente di configurazione.

8.2. Impostazioni di sicurezza

In questa area, è possibile abilitare o disabilitare le impostazioni del prodotto che riguardano vari aspetti della sicurezza del computer e dei dati. Lo stato attuale delle impostazioni è indicato usando una di queste icone:

Cerchio verde con un segno di spunta: L'impostazione è abilitata.

Cerchio rosso con un punto esclamativo: L'impostazione è disabilitata.

Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

Avvertimento

Prestare molta attenzione prima di disabilitare la protezione antivirus in tempo reale o aggiornamenti automatici. Disabilitare queste funzionalità potrebbe compromettere la sicurezza del proprio computer. Se è davvero necessario disabilitarle, ricordarsi di riabilitarle appena possibile.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Antivirus	La protezione in tempo reale assicura che tutti i file vengano scansionati quando l'utente o un'applicazione eseguita nel sistema vi accede.
Aggiornamento automatico	L'aggiornamento automatico assicura che la versione più recente del prodotto BitDefender e i file di firma vengano scaricati ed installati automaticamente e regolarmente.
Controllo Vulnerabilità	Il controllo automatico delle Vulnerabilità assicura che il software cruciale del computer sia aggiornato.
Antiphishing	L'Antiphishing rileva se una pagina web è impostata per rubare informazioni personali e avverte in tempo reale.
Controllo Identità	Il Controllo identità consente di impedire la diffusione dei propri dati personali su Internet senza il proprio consenso. Impedisce che messaggi immediati, e-mail o moduli web trasmettano dati definiti come privati a destinatari (indirizzi) non autorizzati.

Impostazione	Descrizione
Criptazione dell'IM	La Criptazione IM (Instant Messaging) rende sicure le conversazioni via Yahoo! Messenger e Windows Live Messenger a patto che i contatti IM usino un prodotto compatibile con BitDefender e software IM.

Lo stato di alcune di queste impostazioni può essere monitorato dal sistema di controllo dei problemi di BitDefender. Se viene disabilitata una impostazione controllata, BitDefender segnalerà un problema che deve essere risolto.

Se non si desidera che le impostazioni di monitoraggio disabilitate vengano indicate come problemi, è necessario configurare di conseguenza il sistema di monitoraggio. È possibile far ciò nella Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio è configurato da posizioni separate, a seconda delle categorie di impostazioni. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 72) di questo manuale.
- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura stato monitoraggio**.
  3. Deselezionare la casella di spunta corrispondente alle voci che non si desidera monitorare.

  Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 95).

8.3. Impostazioni generali

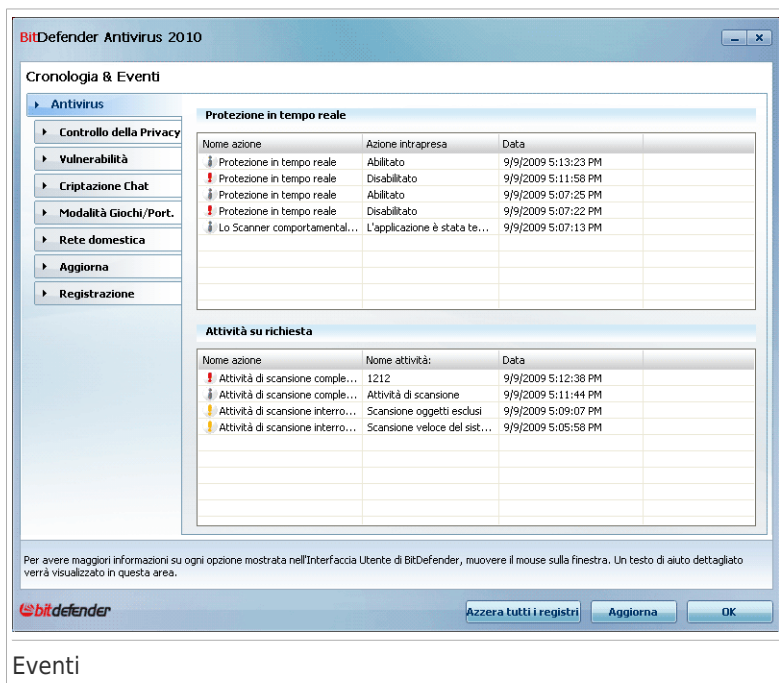
In questa area, è possibile abilitare o disabilitare impostazioni che influenzano il comportamento del prodotto e l'esperienza utente. Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Modalità Gioco	La Modalità giochi modifica temporaneamente le impostazioni di protezione in modo da minimizzare il loro impatto sulle performance del sistema durante le sessioni di gioco.
Rilevamento Modalità portatile	La Modalità Portatile modifica temporaneamente le impostazioni di protezione in modo da minimizzare il

Impostazione	Descrizione
	loro impatto sulla durata della batteria del computer portatile.
Password delle impostazioni	Questo assicura che le impostazioni di BitDefender possano essere modificate solo da una persona che conosca questa password. Quando viene abilitata questa opzione verrà richiesto di configurare la password impostazioni. Digitare la password desiderata in entrambi i campi e fare clic su **OK** per impostare la password.
Notizie BitDefender	Abilitando questa opzione, riceverete da BitDefender importanti notizie sull'azienda, aggiornamenti del prodotto e notizie sulle nuove minacce per la sicurezza.
Avvisi notifiche prodotto	Abilitando questa opzione riceverete informazioni sugli allarmi.
Barra dell'Attività di scansione	La Barra dell'attività di scansione è una piccola finestra trasparente che indica l'avanzamento dell'attività dell'attività di scansione di BitDefender. Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 30).
Inviare report sui Virus	Abilitando questa opzione i report sulle scansioni antivirus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.
Rilevamento di Outbreak	Abilitando questa opzione i report riguardanti potenziali outbreak di virus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.

9. Cronologia ed Eventi

Il link **Visualizza Registri** nella parte inferiore della finestra principale di BitDefender apre un'altra finestra che visualizza la cronologia e gli eventi di BitDefender. Tale finestra offre una panoramica di tutti gli eventi relativi alla sicurezza. Per esempio, potete potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato rilevato del malware sul vostro computer, etc.

Eventi

Per aiutarvi a filtrare la cronologia ed eventi di BitDefender, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Controllo della Privacy**
- **Vulnerabilità**
- **Criptazione IM**
- **Modalità portatile/giochi**
- **Rete Domestica**
- **Aggiornamento**
- **Registrazione**

Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da BitDefender quando è successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

Fare clic su **Cancella tutti i registri** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiorna** per assicurarsi di visualizzare i registri più recenti.

10. Registrazione e Il mio Account

BitDefender Antivirus 2010 ha un periodo di prova di 30 giorni. Durante il periodo di prova il prodotto è dotato di tutte le funzionalità e può essere valutato per verificare se risponde alle vostre aspettative. Si noti che dopo 15 giorni di valutazione il prodotto cessa gli aggiornamenti a meno che non venga creato un account BitDefender. Creare un account BitDefender è parte obbligatoria del processo di registrazione

Prima del termine del periodo di prova è necessario registrare il prodotto per mantenere il computer protetto. La registrazione è una procedura in due fasi:

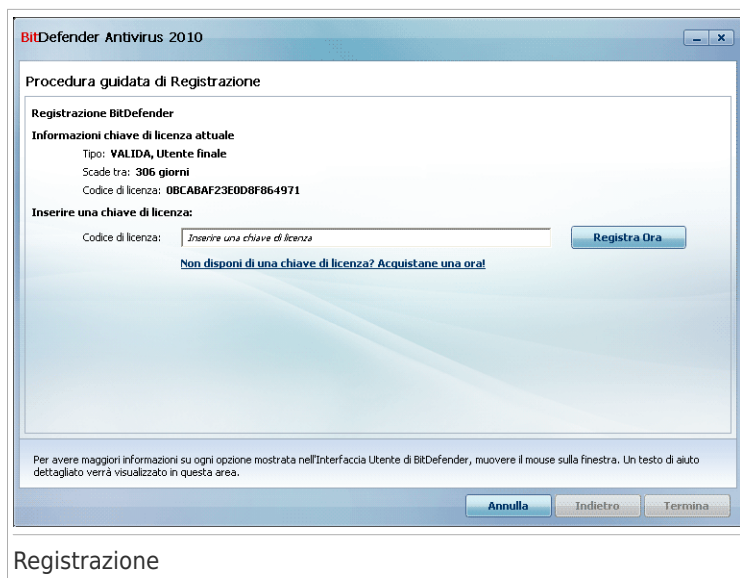
1. **Attivazione del prodotto (registrazione di un account BitDefender).** E' necessario creare un account BitDefender per poter ricevere gli aggiornamenti ed avere accesso all'assistenza tecnica gratuita. Se si dispone già di un account BitDefender, è possibile registrare il prodotto BitDefender con tale account. BitDefender notificherà la necessità di attivare il prodotto e aiuterà a risolvere tale problema.

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

2. **Registrazione con una chiave di licenza.** La chiave di licenza specifica la durata di tempo per cui siete autorizzati ad utilizzare il prodotto. Non appena la chiave di licenza scade BitDefender cessa di eseguire le sue funzioni e di proteggere il computer. E' necessario registrare il prodotto con una chiave di licenza valida alla scadenza del periodo di prova. E' preferibile acquistare o rinnovare una chiave di licenza alcuni giorni prima della scadenza della chiave di licenza attuale.

10.1. Registrazione di BitDefender Antivirus 2010

Se si desidera registrare il prodotto con una chiave di licenza oppure modificare la chiave di licenza attuale, fare clic sul link **Registra Ora** situato nella parte inferiore della finestra BitDefender. Apparirà la finestra di registrazione del prodotto.

Registrazione

Potete vedere lo stato della registrazione BitDefender, la chiave di licenza corrente ed i giorni mancanti alla scadenza della licenza.

Per registrare BitDefender Antivirus 2010:

1. Inserire la chiave di licenza nel campo di modifica.

Nota

Potete trovare la vostra chiave di licenza:
- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

2. Fare clic su **Registra Ora**.
3. Selezionare **Termina**.

10.2. Attivazione di BitDefender

Per attivare BitDefender, è necessario creare o accedere ad un account BitDefender. Se non si è effettuata la registrazione ad un account BitDefender durante l'assistente di registrazione iniziale, è possibile farlo nel modo seguente:

- In Modalità Inesperto, fare clic su **Risolvi Tutti i Problemi**. L'assistente permetterà di risolvere tutti i problemi in sospeso, inclusa l'attivazione del prodotto.
- In Modalità Intermedia, andare alla scheda **Sicurezza** e fare clic sul pulsante **Risolvi** corrispondente al problema relativo all'attivazione del prodotto.
- In Modalità Avanzata, andare su **Registrazione** e fare clic sul pulsante **Attiva Prodotto**.

Si aprirà la finestra di registrazione dell'account. Qui è possibile creare o accedere ad un account BitDefender per attivare il prodotto.

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 51)
- «Ho già un account BitDefender» (p. 51)

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.
   - **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
   - **Confermare Password** - inserire di nuovo la password specificata previamente.

Nota
Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Nota
Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

10.3. Acquisto di chiavi di licenza

Se il periodo di prova è quasi in scadenza, è necessario acquistare una chiave di licenza e registrare il prodotto. Aprire BitDefender e fare clic sul link **Acquista/Rinnova**, posizionato nella parte inferiore della finestra. Il collegamento apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto BitDefender.

10.4. Rinnovo della Licenza

In quanto clienti BitDefender, avete diritto ad uno sconto quando viene rinnovata la licenza del vostro prodotto BitDefender. E' anche possibile aggiornare il prodotto alla versione più recente con uno sconto speciale o gratuitamente.

Se la chiave di licenza attuale è quasi in scadenza, è necessario rinnovare la licenza. Aprire BitDefender e fare clic sul link **Acquista/Rinnova**, posizionato nella parte inferiore della finestra. Il collegamento apre una pagina web dove è possibile rinnovare la licenza.

11. Procedure guidate

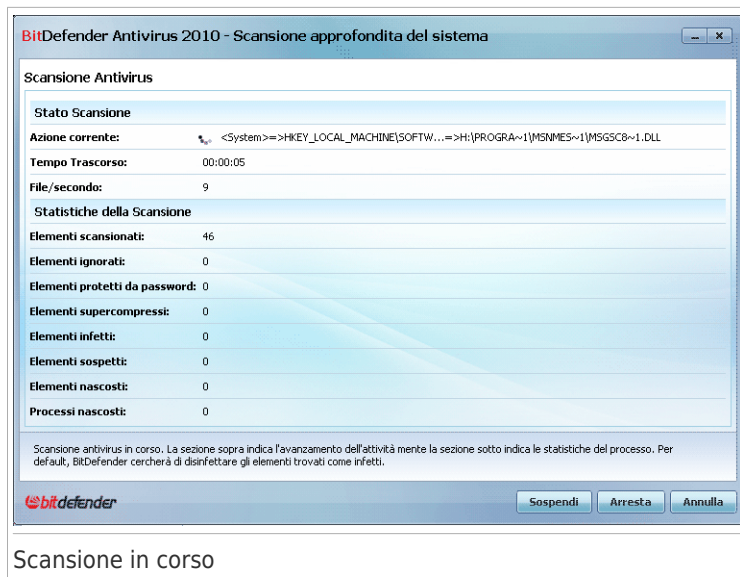
Per facilitare l'uso di BitDefender, diverse procedure guidate aiutano a svolgere specifiche attività di sicurezza o configurare impostazioni del prodotto più complesse. Questa capitolo descrive le procedure guidate potrebbero apparire quando si risolvono problemi o svolgono attività specifiche con BitDefender. Altre procedure guidate di configurazione sono descritte separatamente nella parte «Modalità avanzata» (p. 94).

11.1. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, facendo clic con il tasto destro su una cartella e selezionando **Scansiona con BitDefender**), apparirà l'assistente Scansione Antivirus BitDefender. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

11.1.1. Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che BitDefender finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se BitDefender rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Desidero inserire la password per questo oggetto.** Se si desidera che BitDefender scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non desidero inserire la password per questo oggetto (ignora questo oggetto).** Selezionare questa opzione per non scansionare questo archivio.
- **Non desidero inserire la password per questi oggetti (ignora tutti gli oggetti protetti da password).** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli archivi protetti da password. BitDefender non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

11.1.2. Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire

Azione	Descrizione
	il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

11.1.3. Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

Riassunto

E’ possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante

Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

BitDefender potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.it. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

BitDefender ha rilevato dei file sospetti.

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab BitDefender. Cliccare su **OK** per inviare questi file ai laboratori BitDefender per ulteriori analisi.

11.2. Assistente Scansione Personalizzata

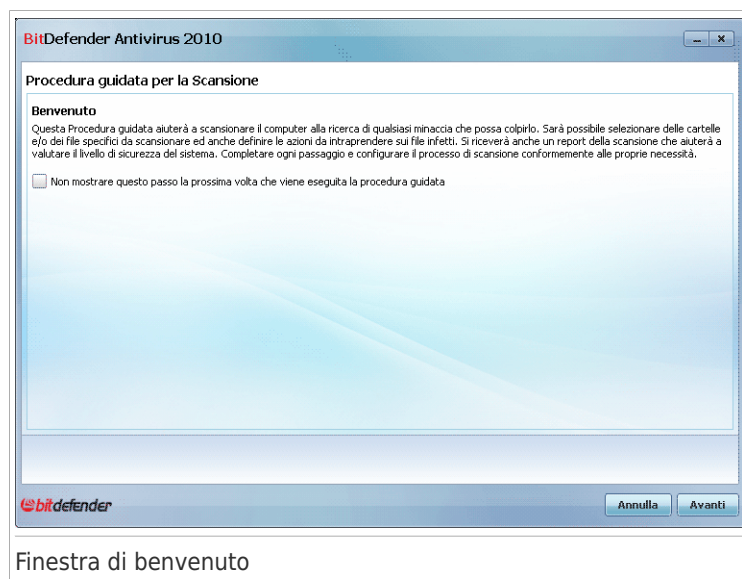
L'Assistente Scansione Personalizzata vi permette di creare ed eseguire un'attività di scansione personalizzata e di salvarla opzionamente come Attività Veloce quando si utilizza BitDefender in Modalità Intermedia.

Per eseguire un'attività di scansione personalizzata utilizzando l'Assistente Scansione Personalizzata, è necessario seguire questi passi:

1. In Modalità Intermedia, andare alla scheda **Antivirus**.
2. Nell'area Funzioni Rapide, clicca **Scansione Personalizzata**.
3. Seguire i sei passi della procedura guidata per completare il processo di scansione.

11.2.1. Passo 1/6 - Finestra di Benvenuto

Questa è una finestra di benvenuto.

Finestra di benvenuto

Se si desidera ignorare questa finestra quando si esegue di nuovo l'assistente in futuro, selezionare la casella di controllo **Non mostrare questo passo la prossima volta che viene eseguito l'assistente**.

Selezionare **Avanti**.

11.2.2. Passo 2/6 - Selezionare Target

Qui è possibile specificare i file o le cartelle da scansionare, nonché le opzioni di scansione.

Selezionare Target

Fare clic su **Aggiungere Target**, selezionare i file o le cartelle che si desidera scansionare e fare clic su **OK**. I percorsi alle posizioni selezionate appariranno nella colonna **Target di scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutto** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si è conclusa la selezione delle posizioni, impostare le **Opzioni di Scansione**. Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Tutti i file	Selezionare questa opzione per esaminare tutti i file nelle cartelle desiderate.
Scansiona solo i file con estensioni di applicazione	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`;

Opzione	Descrizione
	.hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
Esamina solo le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

Selezionare **Avanti**.

11.2.3. Passo 3/6 - Selezionare Azioni

Qui è possibile specificare le impostazioni dello scanner e il livello di scansione.

Selezionare Azioni

- Selezionare le azioni da intraprendere sui file infetti e sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.

Azione	Descrizione
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- Selezionare l'azione da intraprendere sui file nascosti (rootkit). Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.

- Configurare l'aggessività dello scanner. Vi sono 3 livelli da cui scegliere. Trascinare il selettore lungo la scala per impostare il livello di protezione più adeguato:

Livello di scansione	Descrizione
Permissiva	Vengono esaminate solo le applicazioni e solo alla ricerca di virus. Il livello di consumo delle risorse è basso.
Default	Il livello di consumo delle risorse è moderato. Vengono analizzati tutti i file alla ricerca di virus e spyware.
Aggressiva	Vengono esaminati tutti i file (inclusi gli archivi) alla ricerca di virus e spyware. I file nascosti e i processi sono inclusi nella scansione. Il livello di consumo delle risorse è elevato.

Gli utenti più esperti possono trarre vantaggio dalle impostazioni di scansione offerte da BitDefender. Lo scanner può essere impostato per la ricerca di minacce malware specifiche. Questo può ridurre considerevolmente i tempi di scansione e migliorare i tempi di risposta del computer durante la scansione.

Trascinare il selettore per selezionare **Personalizzazione** quindi fare clic sul pulsante **Livello di Personalizzazione**. Apparirà una finestra. Specificare il tipo di malware per cui si desidera che BitDefender compia una scansione selezionando le opzioni appropriate:

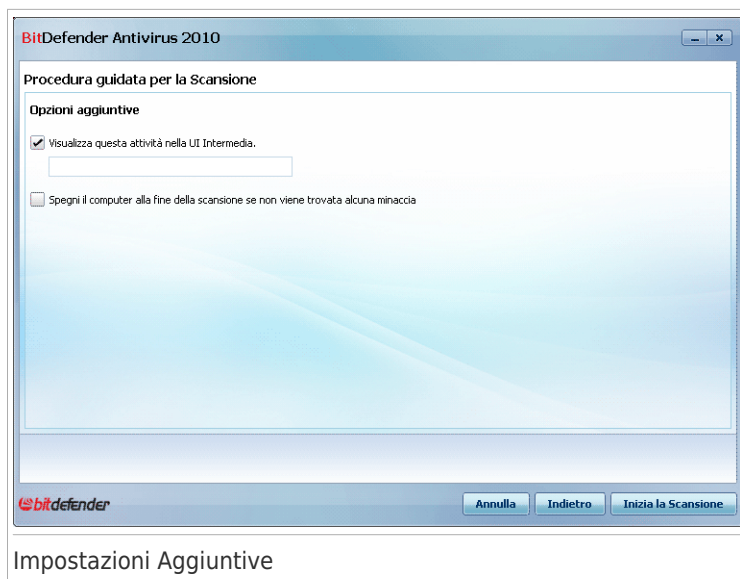
Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansiona alla ricerca di applicazioni	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.
Scansiona alla ricerca di keylogger	Scansiona applicazioni malevole che registrano i tasti premuti.

Selezionare **OK** per chiudere la finestra.

Selezionare **Avanti**.

11.2.4. Passo 4/6 - Impostazioni Aggiuntive

Prima dell'avvio della scansione sono disponibili alcune opzioni aggiuntive:

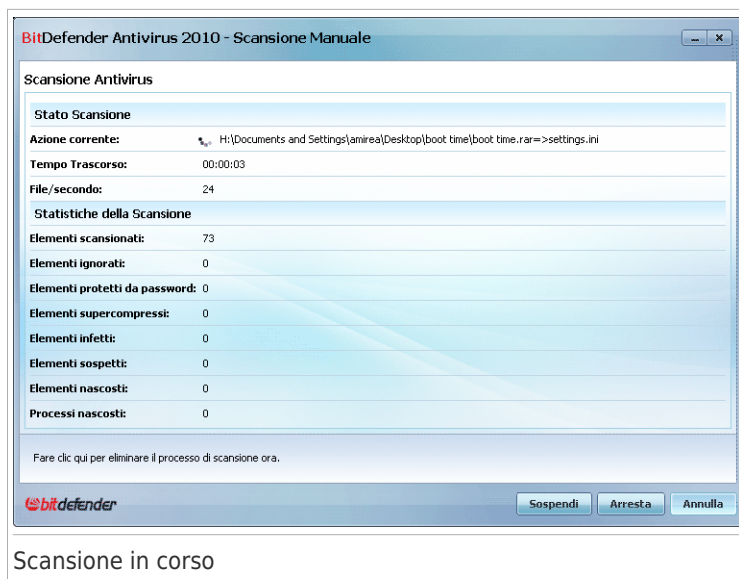
Impostazioni Aggiuntive

- Per salvare l'attività personalizzata che si sta creando per l'uso in futuro, selezionare la casella di controllo **Mostra questa attività nell'Interfaccia Utente Intermedia** ed inserire il nome dell'attività nel campo di immissione fornito.

  L'attività verra aggiunta all'elenco di Attività Veloci disponibile alla scheda Sicurezza e apparirà anche in **Modalità Avanzata > Antivirus > Scansione Virus**.
- Per spegnere il computer quando la scansione è completata, selezionare la casella di controllo **Spegnere il computer quando la scansione è terminata se non sono state individuate minacce**.

Fare clic su **Avvia Scansione**.

11.2.5. Passo 5/6 - Scansione

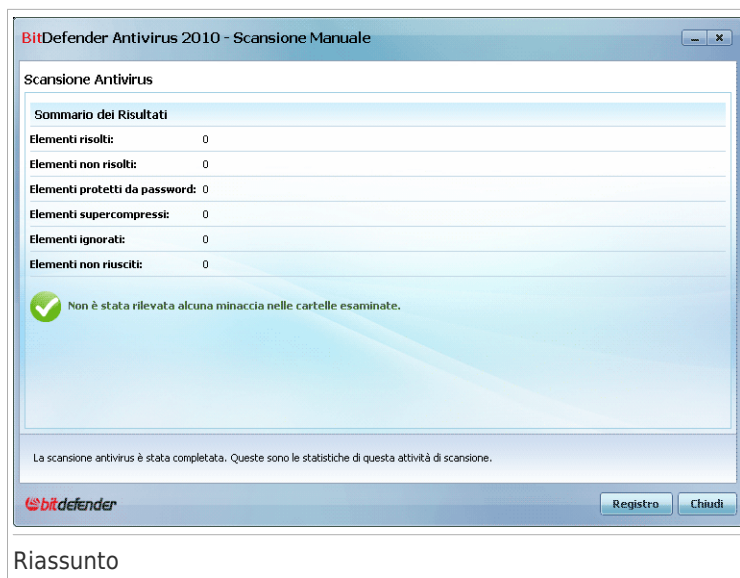
BitDefender inizierà la scansione degli oggetti selezionati:

Scansione in corso

Nota

La durata del processo dipende dalla complessità della scansione. Facendo clic sull'icona di avanzamento della scansione nell'area di notifica si aprirà la finestra di scansione e sarà possibile osservare l'avanzamento della scansione.

11.2.6. Passo 6/6 – Visualizzare Risultati

Quando BitDefender completa il processo di scansione, i risultati della scansione verranno visualizzati in una nuova finestra:

Riassunto

Viene visualizzato il riepilogo dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza Registro** per visualizzare il registro di scansione.

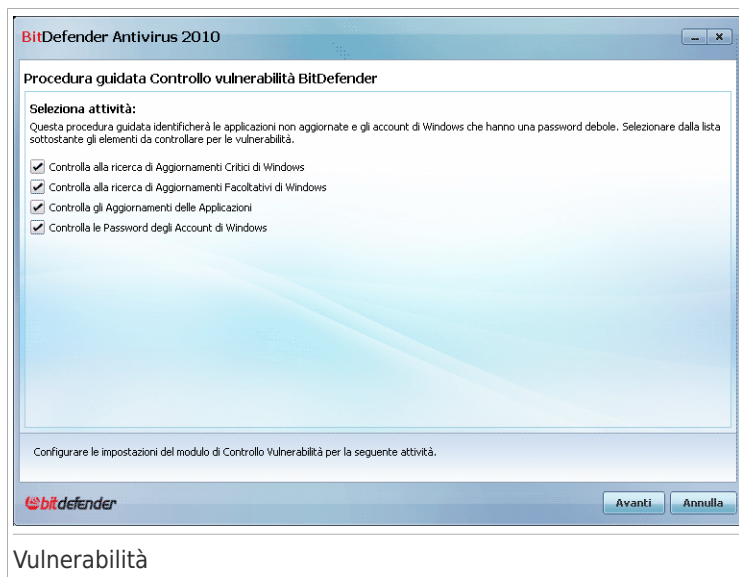
Importante

Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

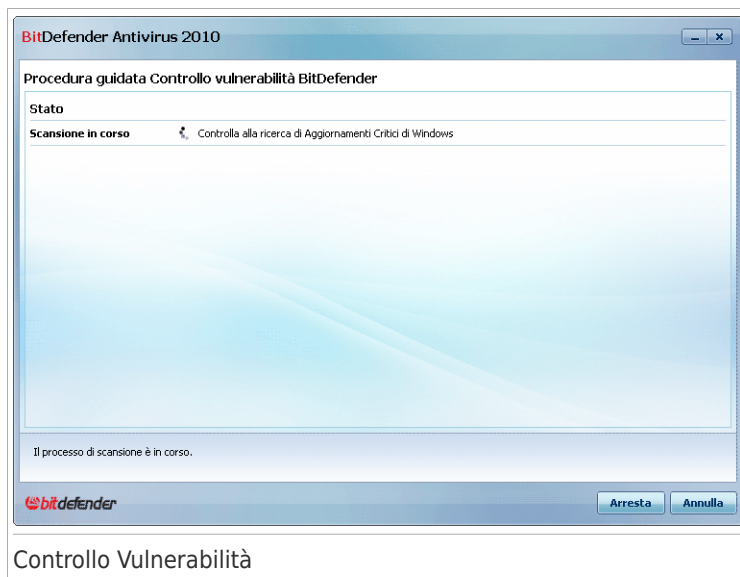
11.3. Procedura guidata di Controllo delle vulnerabilità

L'assistente controlla le vulnerabilità del sistema e permette di risolverle.

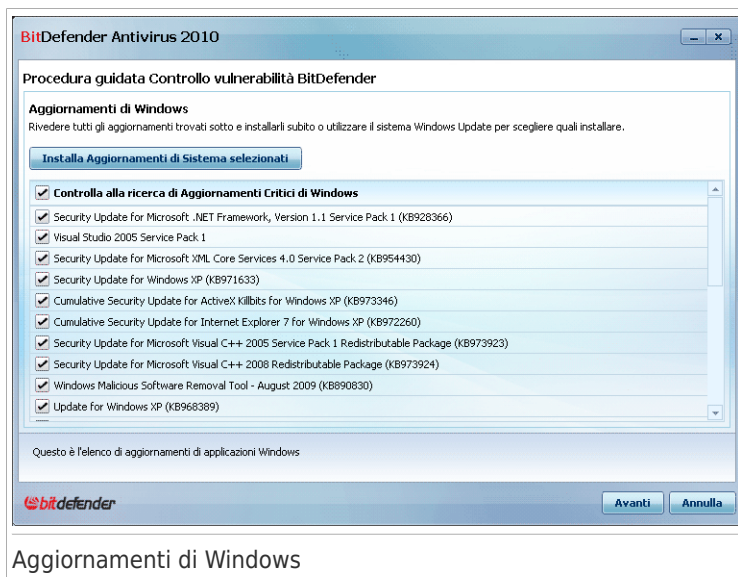
11.3.1. Passo 1/6 – Selezionare le Vulnerabilità da controllare.

Vulnerabilità

Cliccare su **Avanti** per esaminare il sistema alla ricerca delle vulnerabilità selezionate.

11.3.2. Passo 2/6 - Controllare Vulnerabilità

Controllo Vulnerabilità

Attendere che BitDefender finisca il controllo alla ricerca di vulnerabilità.

11.3.3. Passo 3/6 - Aggiornare Windows

Aggiornamenti di Windows

Potete vedere l'elenco degli aggiornamenti critici e non critici di Windos che non sono attualmente installati sul computer. Clicare su **Installare tutti gli aggiornamenti di sistema** per installare tutti gli aggiornamenti disponibili.

Selezionare **Avanti**.

11.3.4. Passo 4/6 - Aggiornare le Applicazioni

Applicazioni

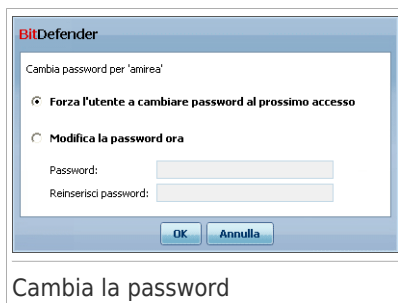
Potete vedere l'elenco di tutte le applicazioni controllate da BitDefender e se sono aggiornate. Se un'applicazione non è aggiornata, cliccare sul link fornito per scaricare la versione più recente.

Selezionare **Avanti**.

11.3.5. Passo 5/6 - Cambiare password deboli

Password dell'utente

Potete visualizzare l'elenco degli account di Windows configurati sul vostro computer ed il livello di protezione che le loro password forniscono. Una password può essere **forte** (difficile da indovinare) o **debole** (facile da indovinare da persone malvagie con software specializzati).

Cliccare su **Risolvere** per modificare le password deboli. Apparirà una nuova finestra.

Cambia la password

Selezionare il metodo per risolvere questo problema:

- **Forza l'utente a cambiare password al prossimo accesso.** BirDefender chiederà l'utente di cambiare la password la prossima volta che acceda a Windows.

- **Cambia password dell'utente.** Devi inserire la nuova password nei campi corrispondenti. Assicurarsi di informare l'utente in merito al cambiamento della password.

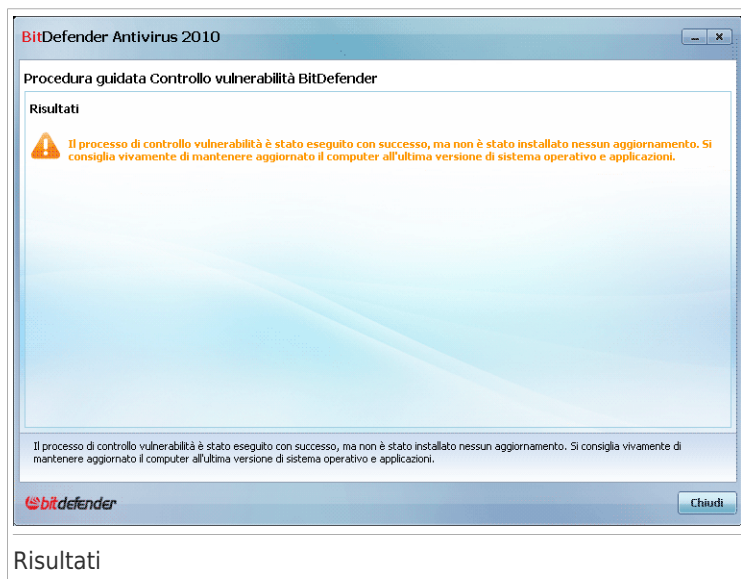
Nota

Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @). È possibile eseguire una ricerca su Internet per ulteriori informazioni e consigli sul creare forti password.

Cliccare su **OK** per cambiare la password.

Selezionare **Avanti**.

11.3.6. Passo 6/6 – Visualizzare Risultati

Risultati

Cliccare su **Chiudere**.

Modalità intermedia

12. Dashboard

La scheda Dashboard fornisce informazioni sullo stato di sicurezza del computer e permette di risolvere i problemi in sospeso.

Dashboard

La Dashboard è costituita dalle seguenti sezioni:

- **Stato Generale** - Indica il numero di problemi che influiscono sul computer ed aiuta a risolverli. Se vi sono problemi in sospeso verrà visualizzato un **cerchio rosso con un punto esclamativo** e il pulsante **Risolvi Tutti i Problemi**. Fare clic sul pulsante per avviare l'assistente Risolvi Tutti i Problemi.
- **Dettagli Stato** - Indica lo stato di ciascun modulo principale utilizzando frasi esplicite e una delle seguenti icone:

  Cerchio verde con un segno di spunta: Non vi sono problemi che influenzano lo stato di sicurezza. Il computer e i dati sono protetti.

  Cerchio grigio con un punto esclamativo: L'attività dei componenti di questo modulo non viene monitorata. Di conseguenza non vi sono informazioni disponibili sullo stato di sicurezza di tali componenti. Potrebbero esservi problemi specifici relativi a questo modulo.

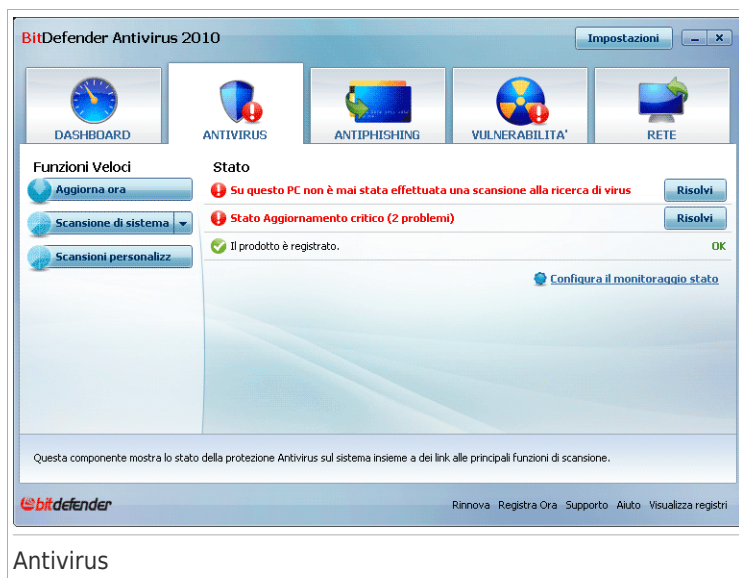
  Cerchio rosso con un punto esclamativo: Vi sono problemi che influiscono sulla sicurezza del sistema. I problemi critici richiedono immediata attenzione. Anche i problemi non critici dovrebbero essere affrontati il più presto possibile.

Fare clic sul nome di un modulo per visualizzare ulteriori dettagli sul suo stato e per configurare il monitoraggio dello stato dei suoi componenti.

- **Profilo di Utilizzo** - Indica il profilo di utilizzo attualmente selezionato e offre link alle attività collegate a tale profilo:
  - Quando è selezionato il profilo **Tipico** il pulsante **Scansione Ora** permettere di compiere una scansione del sistema utilizzando l'Assistente Scansione Antivirus. Verrà esaminato l'intero sistema, con l'eccezione degli archivi. Nella configurazione di default, viene effettuata la scansione alla ricerca di tutti i tipi di malware eccettuati i rootkit.
  - Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.
  - Quando è selezionato il profilo **Personalizzato** il pulsante **Aggiorna Ora** avvia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.

Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

13. Antivirus

BitDefender contiene un modulo di Antivirus che vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus. Per accedere al modulo Antivirus, cliccare sul tab **Antivirus**.

Antivirus

Il modulo Antivirus ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale di tutti i componenti di sicurezza monitorati e permette di selezionare quali componenti monitorare.
- **Attività Veloci** - Qui si trovano i collegamenti alle attività di sicurezza più importanti: aggiornamento immediato, scansione documenti, scansione del sistema, scansione appprofondita del sistema e scansione personalizzata.

13.1. Area di Stato

L'area di stato visualizza l'elenco completo dei componenti del modulo di sicurezza e il loro stato attuale. Monitorando ogni modulo di sicurezza, BitDefender vi comunicherà non solo quando vengono configurate delle impostazioni che potrebbero influenzare la sicurezza del vostro computer, ma anche quando viene dimenticata l'esecuzione di attività importanti.

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

13.1.1. Configurazione del Monitoraggio Stato

Per selezionare i componenti che BitDefender deve monitorare, fare clic su **Configura Controllo Stato** e selezionare la casella di controllo **Abilita allarmi** corrispondente alle caratteristiche che si desidera monitorare.

Importante

Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

BitDefender può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - BitDefender controlla lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione a richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Questo PC non è stato mai controllato alla ricerca di virus	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - BitDefender controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto BitDefender non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto BitDefender sono obsolete.

13.2. Funzioni Veloci

In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - avvia una scansione completa del computer (archivi esclusi). Per ulteriori attività di scansione a richiesta, fare clic su su questo pulsante e selezionare un'attività di scansione differente: Scansione Documenti o Scansione Approfondita del Sistema.
- **Scansione Personalizzata** - avvia un assistente che permette di creare ed eseguire un'attività di scansione personalizzata.

13.2.1. Aggiornamento di BitDefender

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Di default, BitDefender controlla se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni ora**. Ad ogni modo, se si vuole aggiornare BitDefender, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:

Aggiornamento di BitDefender

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di BitDefender su richiesta dell'utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

13.2.2. Scansione con BitDefender

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione facendo clic sul pulsante corrispondente o

selezionandolo dal menu a tendina. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Documenti	Usare questa funzione per esaminare le cartelle importanti dell'utente corrente: `Documenti`, `Desktop` e `Avvio`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro e l'esecuzione di applicazioni pulite all'avvio.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Personalizzare Scansione	Usare questa funzione per scegliere file e cartelle specifici da esaminare.

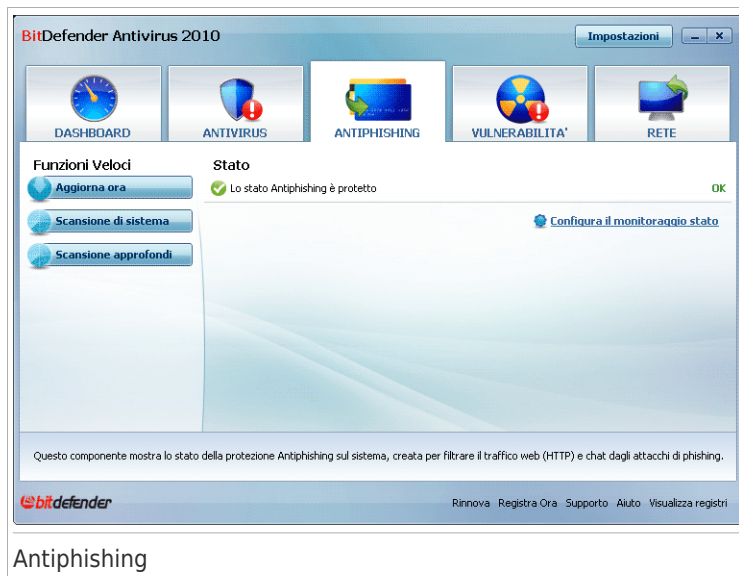
Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

Quando si esegue una Scansione del Sistema, Scansione Approfondita del Sistema o Scansione Documenti, apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

Quando si esegue una Scansione Personalizzata, l'assistente Scansione Personalizzata vi condurrà lungo il processo di scansione. Seguire i sei passi della procedura guidata per effettuare la scansione di file o cartelle specifiche. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Assistente Scansione Personalizzata»* (p. 58).

14. Antiphishing

BitDefender contiene un modulo Antiphishing che assicura che tutte le pagine web a cui si accede tramite Internet Explorer o Firefox siano sicure. Per accedere al modulo Antiphishing, cliccare sul tasto **Antiphishing**.

Antiphishing

Il modulo Antiphishing ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale del modulo antiphishing e permette di abilitare/disabilitare il monitoraggio dell'attività di tale modulo.
- **Attività Veloci** - Qui si trovano i link alle attività di sicurezza più importanti: aggiornamento immediato, scansione del sistema e scansione approfondita del sistema.

14.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato.

Il problema più comune riportato per questo modulo è **Antiphishing disabilitato**. Questo indica che l'Antiphishing non è abilitato per una o più delle seguenti applicazioni supportate: Internet Explorer, Mozilla Firefox, Yahoo! Messenger o Windows Live Messenger.

14.2. Funzioni Veloci

In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
- **Scansione Approfondita del Sistema** - avvia una scansione completa del computer (archivi inclusi).

14.2.1. Aggiornamento di BitDefender

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Di default, BitDefender controlla se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni ora**. Ad ogni modo, se si vuole aggiornare BitDefender, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:

Aggiornamento di BitDefender

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l’aggiornamento periodico di BitDefender su richiesta dell’utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

14.2.2. Scansione con BitDefender

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione facendo clic sul pulsante corrispondente o

selezionandolo dal menu a tendina. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

Quando si esegue una Scansione del Sistema o una Scansione Approfondita del Sistema apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

15. Vulnerabilità

BitDefender contiene un modulo di Vulnerabilità che vi aiuta a mantenere aggiornato il software cruciale sul vostro computer. Per monitorare e risolvere le vulnerabilità del sistema fare clic sulla scheda **Vulnerabilità**.

Vulnerabilità

Il modulo Vulnerabilità ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale del modulo di Controllo Vulnerabilità e permette di abilitare/disabilitare il monitoraggio dell'attività di tale modulo.
- **Attività Veloci** - Qui si trova il link all'assistente controllo vulnerabilità.

15.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** o sul pulsante **Installa** corrispondente ad una frase per risolvere il problema riportato.

I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	BitDefender non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.
Sono state individuate molteplici vulnerabilità	BitDefender ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
`Applicazione` (obsoleta)	È disponibile una nuova versione dell'`Applicazione` ma non è stata installata.
`Utente` (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

15.2. Funzioni Veloci

È disponibile una sola attività:

- **Scansione Vulnerabilità** - avvia una procedura guidata che controlla il sistema alla ricerca di vulnerabilità ed aiuta a risolverle.

La Scansione delle Vulnerabilità controlla gli Aggiornamenti di Microsoft Windows, di Microsoft Windows Office e le password dei tuoi account di Microsoft Windows per assicurare che il tuo Sistema Operativo sia aggiornato e che le password non siano vulnerabili.

Per controllare il computer alla ricerca di vulnerabilità fare clic su **Scansione Vulnerabilità** e seguire l'*«Procedura guidata di Controllo delle vulnerabilità»* (p. 65).

16. Rete

Il modulo Rete vi permette gestire i prodotti BitDefender installati sui computer di casa da un singolo computer. Per accedere al modulo Rete, fare clic sulla scheda **Rete**.

Rete

Per essere in grado di gestire i prodotti BitDefender installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica BitDefender sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).
3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

16.1. Funzioni Veloci

Inizialmente, solo un tasto sarà disponibile.

- **Abilita Rete** - permette di impostare una password di rete, pertanto creando e accedendo ad una rete.

Dopo aversi unito alla rete, appariranno molti più tasti.

- **Disabilita Rete** - permette di lasciare la rete.
- **Aggiungi Computer** - permette di aggiungere computer alla rete.
- **Esaminare Tutti** - vi permette di eseguire la scansione su tutti i computer in gestione contemporaneamente.
- **Aggiornare Tutti** vi permette di aggiornare tutti i computer in gestione contemporaneamente.
- **Registrare Tutti** vi permette di registrare tutti i computer in gestione contemporaneamente.

16.1.1. Unirsi alla Rete BitDefender

Per unirsi alla rete domestica BitDefender, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

16.1.2. Aggiungere dei computer alla Rete BitDefender

Prima di poter aggiungere un computer alla rete domestica BitDefender dovrete configurare la password per la gestione domestica BitDefender sul rispettivo computer.

Per aggiungere un computer alla rete domestica BitDefender , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.

Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

Indica un computer online senza prodotti BitDefender installati.

Indica un computer online con BitDefender installato.

Indica un computer offline con BitDefender installato.

3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.

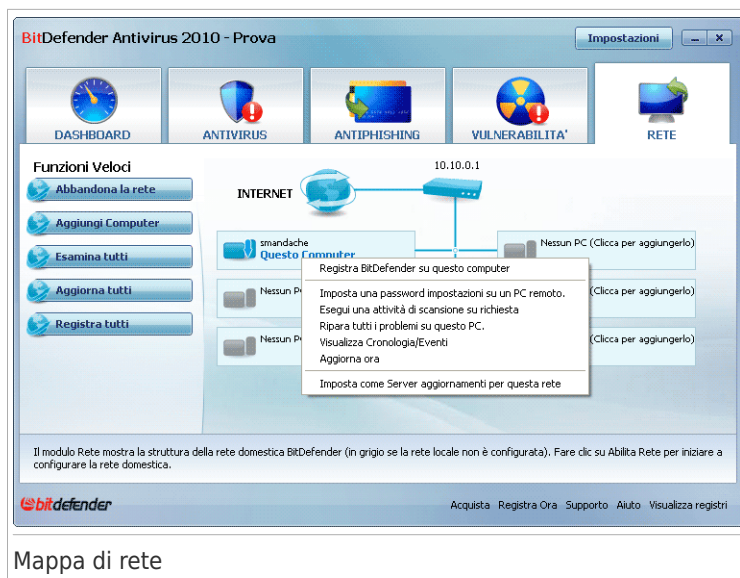
4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.

Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

16.1.3. Gestione della Rete BitDefender

Una volta che avete creato con successo una rete domestica BitDefender, potrete gestire tutti i prodotti BitDefender da un singolo computer.

Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema, stato della registrazione di BitDefender).

Se si fa clic con il pulsante destro sul nome del computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire dal computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Registra BitDefender su questo computer**

  Permette di registrare BitDefender sul computer inserendo una chiave di licenza.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni BitDefender sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi Tutti i Problemi.

- **Visualizzare Cronologia/Eventi**

  Permette di accedere al modulo **Cronologia&Eventi** del prodotto BitDefender installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto BitDefender installato sul computer.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti BitDefender installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

Nota

Se si ha in programma di eseguire diverse funzioni, è possibile selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

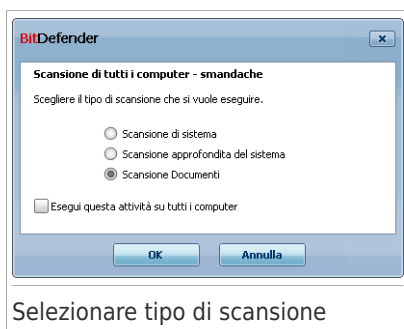
16.1.4. Scansione di tutti i computer

Per esaminare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Esaminare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Selezionare un tipo di scansione.
   - **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
   - **Scansione Approfondita del Sistema** - inizia una scansione completa del computer (archivi inclusi).
   - **Scansione Documenti** - inizia una scansione veloce dei documenti e delle impostazioni.

Selezionare tipo di scansione

3. Selezionare **OK**.

16.1.5. Aggiornamento di tutti i Computer

Per aggiornare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Aggiornare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Selezionare **OK**.

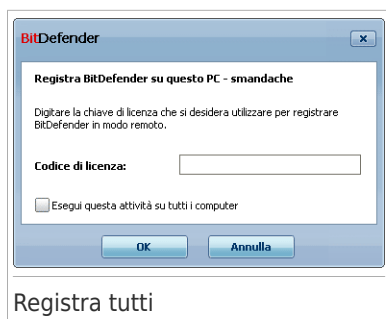
16.1.6. Registrazione di Tutti i Computer

Per registrare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare **Registrare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Inserire la chiave con la quale vi volete registrare.

Registra tutti

3. Selezionare **OK**.

Modalità avanzata

17. Generale

Il modulo Generale fornisce informazioni sull'attività di BitDefender e sul sistema. Qui potete anche modificare il comportamento generale di BitDefender.

17.1. Dashboard

Per visualizzare le statistiche di attività del prodotto, lo stato di registrazione e se vi sono problemi che influiscono sul computer, andare a **Generale>Dashboard** in Modalità Avanzata.

Dashboard

La Dashboard ha diverse sezioni:

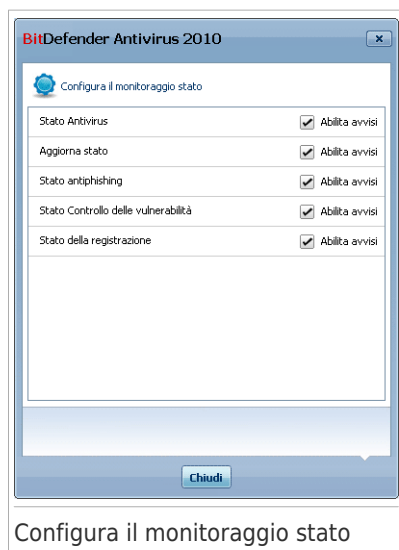
- **Stato Generale** - Informa in merito a qualsiasi problema che influenza la sicurezza del computer.
- **Statistiche** - Mostra importanti informazioni riguardanti l'attività di BitDefender.
- **Informazioni generali** - Mostra lo stato dell'aggiornamento, del vostro account, della registrazione ed informazioni sulla licenza.

- **Attività file** - Indica l'evoluzione del numero di elementi esaminati dall'Antimalware di BitDefender. L'altezza della barra indica l'intensità del traffico durante un intervallo di tempo.

17.1.1. Stato generale

Qui è possibile trovare il numero di problemi che mettono a rischio la sicurezza del computer. Per rimuovere tutte le minacce, fare clic su **Risolvi tutti i problemi**. Questo riavvia la procedura guidata Risolvi tutti i problemi.

Per configurare quali moduli verranno monitorati da BitDefender Antivirus 2010, fare clic su **Configura monitoraggio stato**. Apparirà una nuova finestra:

Configura il monitoraggio stato

Se si desidera che BitDefender monitori un componente, selezionare la casella di controllo **Abilita allarmi** per il componente corrispondente. BitDefender può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - BitDefender monitora lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione su richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.

Problema	Descrizione
Non è mai stata eseguita la scansione del computer alla ricerca di malware	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - BitDefender controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto BitDefender non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto BitDefender sono obsolete.

- **Antiphishing** - BitDefender controlla lo stato della funzione di Antiphishing. Se non è abilitata per tutte le applicazioni supportate, verrà riportato il problema **Antiphishing disabilitato**.
- **Controllo Vulnerabilità** - BitDefender tiene traccia della funzione Controllo Vulnerabilità. Controllo Vulnerabilità comunica all'utente la necessità di installare aggiornamenti di Windows, aggiornamenti dell'applicazione e se è necessario rinforzare alcune password.

  I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	BitDefender non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.

Stato	Descrizione
Sono state individuate molteplici vulnerabilità	BitDefender ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
`Applicazione` (obsoleta)	È disponibile una nuova versione dell'`Applicazione` ma non è stata installata.
`Utente` (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

Importante

Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

17.1.2. Statistiche

Se volete dare un'occhiata all'attività di BitDefender, un buon posto per cominciare è la sezione Statistiche. Potete visualizzare i seguenti elementi:

Elemento	Descrizione
File esaminati	Indica il numero di file che sono stati esaminati alla ricerca di malware al momento dell'ultima scansione.
File disinfettati	Indica il numero dei file che sono stati disinfettati al momento della vostra ultima scansione.
File infettati rilevati	Indica il numero di file infetti che sono stati trovati nel sistema al momento dell'ultima scansione.
Ultima scansione del sistema	Indicata l'ultima scansione del computer. Se l'ultima scansione è stata eseguita più di una settimana fa, eseguire al più presto una nuova scansione. Per eseguire una scansione di tutto il computer, fare clic sulla scheda **Antivirus**, Scansione virus, ed eseguire una Scansione completa di sistema o una Scansione approfondita di sistema.

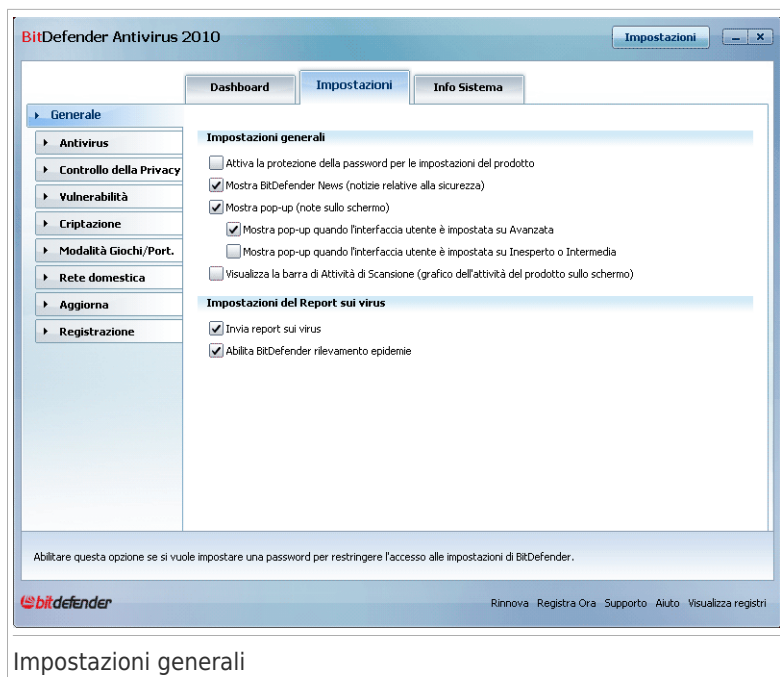
Elemento	Descrizione
Prossima scansione	Indica la prossima volta in cui il computer verrà sottoposto a scansione.

17.1.3. Panoramica

Qui è possibile vedere lo stato di aggiornamento, lo stato dell'account, le informazioni sulla registrazione e la licenza.

Elemento	Descrizione
Ultimo aggiornamento	Indicata quando è stato aggiornato per l'ultima volta il prodotto BitDefender. Eseguire aggiornamenti regolari per avere un sistema completamente protetto.
Account BitDefender	Indica l'indirizzo mail che potrete usare per accedere al vostro account on-line per recuperare la chiave di licenza BitDefender e beneficiare del supporto BitDefender e di altri servizi personalizzati È necessario creare un account BitDefender in modo da attivare il prodotto. Per ulteriori informazioni sull'account BitDefender, fare riferimento a *«Registrazione e Il mio Account»* (p. 48).
Registrazione	Indica il tipo e lo stato della vostra chiave di licenza. Per mantenere sicuro il vostro sistema dovete rinnovare o aggiornare BitDefender se la vostra chiave è scaduta.
Scade in	Indica il numero di giorni che mancano alla scadenza della chiave di licenza. Sa la chiave di licenza scade entro qualche giorno, registrare il prodotto con una nuova chiave di licenza. Per acquistare una chiave di licenza o rinnovare la licenza, fare clic sul link **Acquista/Rinnova**, situato in basso nella finestra.

17.2. Impostazioni

Per configurare e gestire le impostazioni generali di BitDefender andare su **Generale>Impostazioni** in Modalità Avanzata.

Impostazioni generali

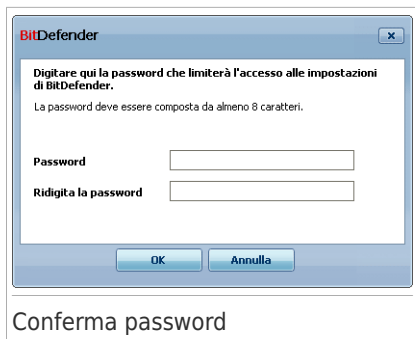
Da qui è possibile impostare il comportamento generale di BitDefender. BitDefender è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

17.2.1. Impostazioni generali

- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione di BitDefender.

Nota
Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password.

Selezionando questa opzione, apparirà la seguente finestra:

Conferma password

Digitare la password nel campo **Password**, quindi re-inserirla nel campo **Ridigitare password** e selezionare **OK**.

Una volta che avete impostato la password, vi verrà chiesta ogni volta che vorrete cambiare le impostazioni di BitDefender. Gli altri amministratori del sistema (se ci sono) dovranno anche loro fornire questa password per cambiare le impostazioni di BitDefender.

Importante

Se si dimentica la password, si deve riparare il prodotto per modificare la configurazione BitDefender.

- **Ricezione notifiche di sicurezza** - riceve di volta in volta, dai server BitDefender, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Mostra pop-ups (attiva la schermata delle note)** - mostra finestre a tendina relative allo stato del prodotto. È possibile configurare BitDefender affinché visualizzi pop-up solo quando l'interfaccia è nella Modalità Inesperto / Intermedia o nella Modalità Avanzata.
- **Vusalizza barra di attività della scansione (grafico dell'attività del prodotto a schermo)** - mostra la barra delle Attività della Scansione ogni volta che si accede a Windows. Deselezionare la casella se non volete che la barra delle Attività di Scansione venga mostrata ancora.

Barra di Attività della Scansione

Nota

Questa opzione può essere configurata solo per l'account di Windows in uso. La barra dell'attività di scansione è disponibile solo quando l'interfaccia è in Modalità Avanzata.

17.2.2. Impostazioni del Report sui virus

- **Invia rapporti dei virus** - invia ai Laboratori BitDefender i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

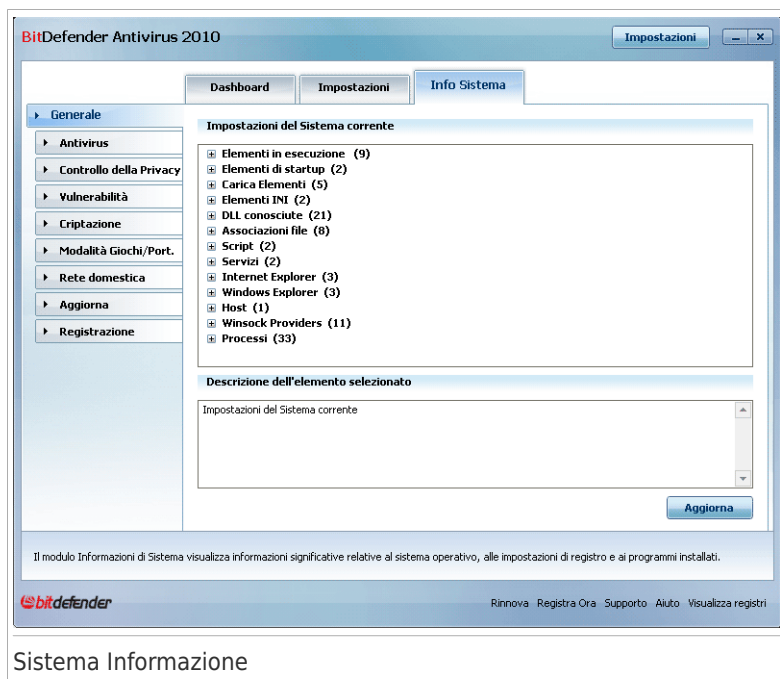
I rapporti non contengono dati confidenziali, come il vostro nome, l’indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare rapporti statistici.

- **Attivare Outbreak Detection BitDefender** - invia ai Laboratori BitDefender i report relativi al potenziale scoppio di un virus.

  I report non contengono dati confidenziali, come il vostro nome, l’indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno esclusivamente il nome del virus e verranno utilizzate per creare report statistici.

17.3. Sistema Informazione

BitDefender vi permette di visualizzare, da una singola ubicazione, tutta la configurazione del sistema e le applicazioni che verranno eseguite all'avvio. In questo modo potrete monitorare l'attività del sistema e delle applicazioni installate così come identificare possibili infezioni del sistema.

Per ottenere informazioni sul sistema, cliccare su **Generale>Informazioni di Sistema** in Modalità Avanzata.

Sistema Informazione

La lista contiene tutti gli elementi caricati quando si avvia il sistema oltre agli elementi caricati da varie applicazioni.

Tre pulsanti sono disponibili:

- **Ripristinare** - Cambia l'associazione di un file corrente a quella di default. Disponibile solo per le impostazioni delle **Associazioni File**!
- **Vai a** - apri una finestra dove l'elemento selezionato è situato (la **Registrazione** ad esempio).

Nota
A seconda dell'elemento selezionato, il pulsante **Vai a** potrebbe non apparire.

- **Aggiorna** - riapri la sezione del **Sistema Informazione** section.

18. Antivirus

BitDefender protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro). La protezione che BitDefender vi offre è divisa in due categorie:

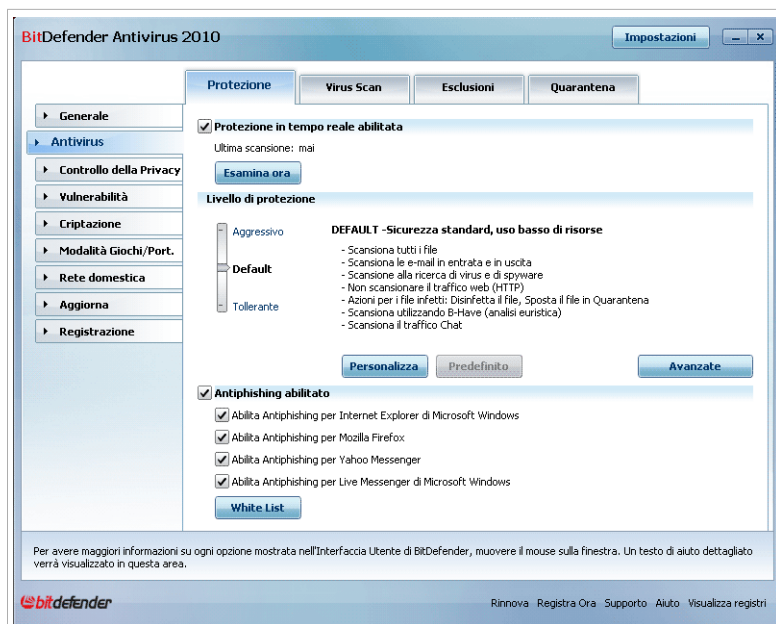
- Protezione in tempo reale - previene l'ingresso di nuove minacce malware nel vostro sistema. BitDefender esaminerà, ad esempio, un documento word quando verrà aperto, ed una mail quando verrà ricevuta.

Nota
La protezione in tempo reale si riferisce anche alla scansione "all'accesso" - i file vengono esaminati nel momento in cui gli utenti vi accedono.

- Scansione a richiesta - permette di rilevare e di rimuovere malware già residente nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta. I processi della scansione vi permettono di creare routine di scansione personalizzate e la loro esecuzione può essere programmata con una cadenza regolare.

18.1. Protezione in tempo reale

BitDefender fornisce una continua protezione in tempo reale contro un ampio spettro di minacce malware mediante la scansione di tutti i file nei quali si è effettuato l'accesso, le mail e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). BitDefender Antiphishing vi impedisce di svelare informazioni personali mentre navigate su internet avvertendovi delle potenziali pagine web con phishing.

Per configurare la protezione in tempo reale e BitDefender Antiphishing, fare clic su **Antivirus>Shield** in Modalità Avanzata.

Protezione in tempo reale

Potete vedere se la Protezione in tempo reale è abilitata o disabilitata. Se volete cambiare lo stato della Protezione in tempo reale, selezionare o deselezionare la casella corrispondente.

Importante
Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Per avviare una scansione del sistema, fare clic su **Scansiona Ora**.

18.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

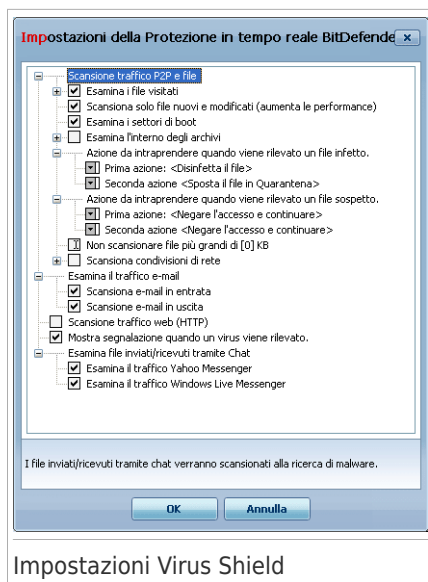
Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso. Solo i programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Default	Offre una sicureza standard. Il livello di consumo delle risorse è basso. Tutti i file e i messaggi di posta in arrivo ed in uscita sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Aggressiva	Offre una sicurezza alta. Il livello di consumo delle risorse è moderato. Tutti i file, e i messaggi e-mail in entrata ed in uscita ed il traffico web sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.

Per applicare le impostazioni di protezione in tempo reale di default cliccare su **Livello di Default**.

18.1.2. Livello di Protezione Personalizzato

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Potete personalizzare la **Real-time protection** cliccando **Custom level**. Apparirà la seguente finestra:

Impostazioni Virus Shield

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Nota
Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate. Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file acceduti e dei transferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

Opzione		Descrizione
Esamina i files acceduti	**Tutti i file**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`;

Opzione		Descrizione
		.doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
	Scansione per riskware	Esamina alla ricerca di riskware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva. Seleziona **Ignora dialer e applicazioni durante la scansione** e/o **Ignora keylogger durante la scansione** se si desidera escludere questi tipi di file dalla scansione.
Scansiona solo i file nuovi e modificati		Scansiona solo i file che non sono stati scansionati in precedenza o che sono stati cambiati dall'ultima scansione. Selezionando questa opzione, è possibile migliorare di molto la risposta generale del sistema con un minimo compromesso per la sicurezza.
Esamina settore di boot		Per esaminare i settori di avvio del sistema.
Esamina gli archivi		Verranno esaminati anche gli archivi acceduti. Con questa opzione abilitata, il computer sarà più lento. È possibile impostare la dimensione massima di archivi da scansionare (in kilobyte, digitare 0 se si vogliono scansionare tutti gli archivi) e la profondità massima di archivi da scansionare.
Prima azione		Seleziona dal menù delle opzioni la prima azione da intraprendere su files infetti o sospetti:
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.

Opzione		Descrizione
	Disinfetta i file	Rimuove il codice malware da file infetti.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Seconda azione		Seleziona la seconda azione dalle opzioni da intraprendere sui files infetti, nel caso in cui la prima fallisse.
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Non scansionare i file più grandi di [x] Kb		Digitare la dimensione massima dei files da esaminare. Se la dimensione è pari a 0 Kb, tutti i files verranno esaminati.
Scansionare condivisioni di rete	**Tutti i file**	Verranno scansionati tutti i file acceduti dalla rete, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` e `.nws`.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

- **Esamina il traffico e-mail** - tutti i messaggi e-mail vengono esaminati.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Esamina le e-mail in ingresso	Tutte le e-mail in ingresso vengono esaminate.
Esamina le e-mail in uscita	Tutte le e-mail in uscita vengono esaminate.

- **Scansiona il traffico web (HTTP)** - tutto il traffico http viene scansionato.
- **Mostra avviso, se viene rilevato un virus** - verrà visualizzata una finestra di avviso quando verrà rilevato un virus in un file o in un messaggio e-mail.

  In presenza di un virus, si aprirà una finestra contenente il nome del virus, e che permetterà di selezionare un azione sul file infetto adottato dal BitDefender, e un link al sito BitDefender dove è possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

  In caso che un file sospetto è scansionati, puoi lanciare un wizard dalla finestra di allerta che ti aiuterà a spedire il file ai Laboratori BitDefender per una ulteriore analisi. È possibile scrivere dalla tua e-mail per ricevere informazioni su questo report.
- **Esamina file ricevuti/inviati tramite IM.** Per esaminare i file che ricevete o inviate usando Yahoo Messenger o Windows Live Messenger, selezionare la casella corrispondente.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

18.1.3. Configurazione Active Virus Control

BitDefender Active Virus Control fornisce un livello di protezione contro nuove minacce le cui firme non sono ancora state rilasciate. Analizza e monitora costantemente il comportamento delle applicazione in esecuzione sul vostro computer e vi avverte se una di queste ha un comportamento sospetto.

AVC può essere configurato per avvisare e richiedere un'azione dell'utente ogni volta che un'applicazione prova a compiere un'azione potenzialmente nociva.

Avviso Active Virus Control

Se conoscete e vi fidate dell'applicazione rilevata, cliccare su **Consentire**.

Se volete chiudere immediatamente l'applicazione, cliccare su **OK**.

Selezionare la casella di controllo **Ricorda questa azione per questa applicazione** prima di eseguire la propria scelta e BitDefender eseguirà la stessa azione per l'applicazione rilevata in futuro. La regola creata viene elencata nella finestra di configurazione Active Virus Control,

Per configurare Active Virus Control, fare clic su **Impostazioni Avanzate**.

Impostazioni Active Virus Control

Selezionare la casella di controllo corrispondente per abilitare Active Virus Control.

Importante

Mantenere Active Virus Control abilitato per essere protetti contro virus sconosciuti.

Se si desidera ricevere avvisi e richieste di azione da parte di Active Virus Control quando una applicazione tenta di eseguire una possibile azione nociva, selezionare la casella di controllo **Chiedi cosa fare**.

Configurazione del Livello di Protezione

Il livello di protezione di AVC cambia automaticamente quando viene impostato un nuovo livello di protezione in tempo reale. Se non siete soddisfatti delle impostazioni di default, potete configurare manualmente il livello di protezione.

Nota

Tenere presente che se viene cambiato il livello corrente di protezione in tempo reale, il livello di protezione di AVC cambierà di conseguenza. Se si imposta la protezione in tempo reale su **Permissiva**, Active Virus Control viene disabilitato automaticamente. In questo caso è possibile abilitarlo manualmente quando si desidera usarlo.

Trascinate il pulsante scorrevole lungo la barra per impostare il livello di protezione che meglio si adatta alle vostre esigenze di sicurezza.

Livello di protezione	Descrizione
Critico	Controllo rigido di tutte le applicazioni alla ricerca di possibili azioni nocive.
Default	Il tasso di rilevamento è elevato e sono possibili dei falsi positivi.
Medio	Controllo dell'applicazione moderato, sono ancora possibili dei falsi positivi.
Permissiva	I tassi di rilevamento sono bassi e non vi sono falsi positivi.

Gestione delle Applicazioni Affidabili / Non affidabili

È possibile aggiungere applicazioni note e affidabili all'elenco di applicazioni affidabili. Queste applicazioni non verranno più controllate da BitDefender Active Virus Control e verrà concesso loro accesso automaticamente.

Le applicazioni per cui sono state create delle regole vengono elencate nella tabella alla voce **Esclusioni**. Per ciascuna regola viene visualizzato il percorso dell'applicazione e l'azione impostata (Permessa o Bloccata).

Per modificare l'azione per un'applicazione fare clic sull'azione attuale e selezionare la nuova azione dal menu.

Per gestire l'elenco utilizzare i pulsanti posizionati al di sotto della tabella:

- **Aggiungi** - per aggiungere una nuova applicazione alla lista.
- **Rimuovi** - per rimuovere una applicazione dalla lista.

- **Modifica** - modifica una regola di applicazione.

18.1.4. Disattivazione Protezione in Tempo Reale

Se volete disattivare la protezione in tempo reale, apparirà la seguente finestra di avviso: Dovrete confermare la vostra scelta selezionando dal menu, per quanto tempo volete disattivare la protezione in tempo reale. Potete disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento

Questa è una questione di sicurezza critica. Vi consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarete protetti dalle minacce malware.

18.1.5. Configurazione della Protezione Antiphishing

BitDefender fornisce protezione antiphishing in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Potete scegliere di disabilitare la protezione antiphishing completamente o solo per applicazioni specifiche.

Potete cliccare su **White List** per configurare e gestire un elenco di pagine web che non devono essere esaminate dai motori Antiphishing BitDefender.

White List Antiphishing

Potete vedere i siti web che BitDefender non controlla attualmente per contenuti phishing.

Per aggiungere un sito alla White List, inserire il suo indirizzo url nel campo corrispondente **Nuovo indirizzo** quindi cliccare **Aggiungi**. La white list dovrebbe contenere solo siti web di cui vi fidate completamente. Ad esempio, aggiungere siti web dove fate di solito i vostri acquisti online.

Nota

Potete aggiungere facilmente dei siti web alla White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nel vostro browser. Per ulteriori informazioni, fare riferimento a *«Integrazione nei Web Browser»* (p. 203).

Per rimuovere un sito web dalla white list, fare clic sul pulsante corrispondente **Rimuovi**.

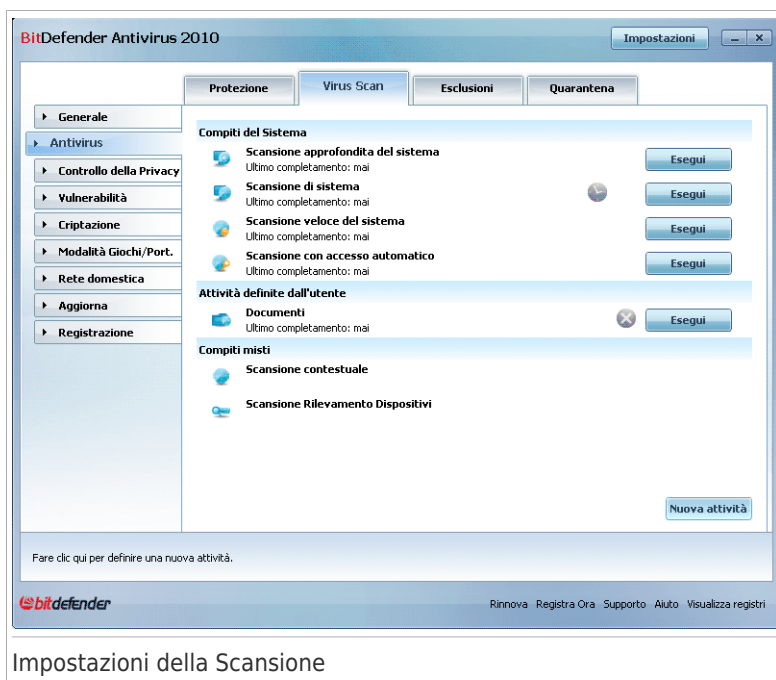
Fare clic su **Salva** per salvare le modifiche e chiudere la finestra.

18.2. Scansione a richiesta

L’obiettivo principale di BitDefender è di mantenere il vostro computer privo di virus. Ciò avviene principalmente tenendo lontani i nuovi virus dal vostro computer ed

esaminando i vostri messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul vostro sistema.

Esiste il rischio che un virus sia già contenuto nel vostro sistema, addirittura prima dell'installazione di BitDefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul vostro computer alla ricerca di virus residenti dopo aver installato BitDefender. inoltre di effettuare frequentemente una scansione del vostro computer alla ricerca di virus.

Per configurare ed avviare la scansione a richiesta, fare clic su **Antivirus>Virus Scan** nella Modalità Avanzata.

Impostazioni della Scansione

La scansione a richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scasione e gli oggetti da esaminare. Potete esaminare il vostro computer in qualsiasi momento, eseguendo le funzioni predefinite oppure le vostre (definite dall'utente). Potete anche programmarle affinchè vengano eseguite con cadenza regolare oppure quando il sistema è inattivo in modo da non interferire con il vostro lavoro.

18.2.1. Impostazioni della Scansione

BitDefender ha tante funzioni, create per default, che coprono i problemi di sicurezza comuni. Voi potete anche creare le vostre funzioni di scansione personalizzate.

Vi sono tre categorie di compiti di scansione:

- **Funzioni di Sistema** - contiene la lista delle funzioni di sistema di default. Sono disponibili i compiti seguenti:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione accesso automatico	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Di default, la scansione autologon è disabilitata Se si vuole utilizzare questa attività, fare clic con il pulsante destro e selezionare **Programma** e impostare l'attività per l'esecuzione **all'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

- **Impostazione Utente** - contiene le impostazioni definite dall'utente.

  Viene fornita una funzione chiamata `My Documents`. Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

- **Compiti misti** - contiene un elenco di compiti di scansione misti. Questi compiti di scansione si riferiscono a tipi di scansione alternativi che non possono essere eseguiti da questa finestra. Potete solo modificare le loro impostazioni o vedere i report delle scansioni.

Ogni attività ha una finestra **Proprietà** che ne permette la configurazione e la visualizzazione dei registri di scansione. Per aprire tale finestra fare doppio clic sul pulsante **Proprietà** prima del nome dell'attività. Per ulteriori informazioni fare riferimento a *«Configurare un Compito di Scansione»* (p. 118).

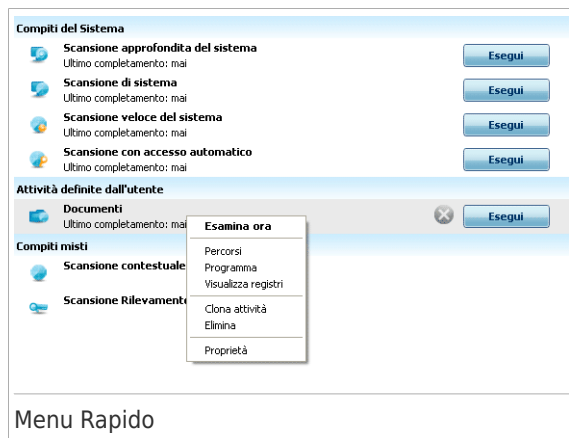
Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Quando un'attività è programmata per essere eseguita automaticamente, in un momento successivo o regolarmente, viene visualizzato il pulsante **Programma** a destra dell'attività. Fare clic su questo pulsante per aprire la finestra **Proprietà**, scheda Programmazione, dove è possibile vedere e modificare il programma dell'attività.

Se non è più necessaria un'attività di scansione creata (definita dall'utente), è possibile cancellare facendo clic sul pulsante **Elimina**, a destra dell'attività. Non è possibile rimuovere attività varie o di sistema.

18.2.2. Utilizzo del Menu Rapido

Un menu rapido è disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.

Menu Rapido

Per le attività di sistema e definite dall'utente sono disponibili i seguenti comandi nel menu di scelta rapida:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Target di Scansione** - apre la sezione Percorso Scansione nella finestra delle **Proprietà**, dove potete cambiare il target di scansione per i compiti selezionati.

Nota
Nel caso di funzioni del sistema, questa opzione viene sostituita da **Mostrare percorsi delle scansioni**, dato che è possibile vedere solo il loro target di scansione.

- **Schedule** - apre la**Finestra proprietà** Programma tab, dove puoi programmare i compiti selezionati.
- **Visualizza registri** - apre la finestra **Proprietà**, scheda Registri dove è possibile vedere i report generati dopo che l'attività selezionata è stata eseguita.
- **Attività di clonazione** - duplica l'attività selezionata. Ciò è utile quando si creano nuovi compiti, in quanto potete modificare le impostazioni del compito duplicato.
- **Cancella** - cancella i compiti selezionati.

Nota
Non disponibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Proprietà** - apre la finestra **Proprietà**, scheda Panoramica, dove è possibile cambiare le impostazioni dell'attività selezionata.

Data la particolare natura della categoria **Attività varie** solo le opzioni **Visualizza registri** e **Proprietà** sono disponibili in questo caso.

18.2.3. Creazione delle Funzioni di Scansione

Per creare un compito di scansione, utilizzare uno di questi metodi:

- Duplica una attività esistente, rinominala ed apporta le modifiche necessarie nella finestra delle Proprietà.
- Cliccare **Nuovo Compito** per creare un nuovo compito e configurarlo.

18.2.4. Configurare un Compito di Scansione

Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per aprire questa finestra fare clic sul pulsante **Proprietà** alla sinistra dell'attività (o fare clic con il pulsante destro sull'attività e poi fare clic su **Proprietà**). E' anche possibile fare doppio clic sull'attività.

Nota
Per ulteriori informazioni sulla visualizzazione dei registri e sulla funzione **Visualizza Registri**, fare riferimento a *«Visualizzazione dei Registri di Scansione»* (p. 138).

Configurazione delle Impostazioni di Scansione

Per configurare le opzioni di scansione di un'attività specifica, fare clic con il pulsante destro e selezionare**Proprietà**. Apparirà la finestra seguente:

Panoramica

Qui potete vedere le informazioni sul compito (nome, ultima esecuzione e stato della programmazione) ed impostare le impostazioni di scansione.

Scelta del Livello di Scansione

Potete facilmente configurare le impostazioni di scansione scegliendo il livello di scansione. Trascinare l'indicatore sulla barra per impostare l'appropriato livello di scansione.

Ci sono 3 livelli di scansione:

Livello di protezione	Descrizione
Permissiva	Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso.

Livello di protezione	Descrizione
	Vengono esaminati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica.
Medio	Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato. Tutti i file vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.
Aggressiva	Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto. Tutti i file e gli archivi vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.

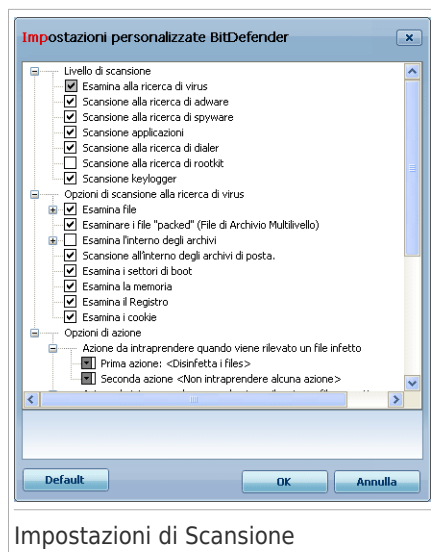
È anche disponibile una serie di opzioni generali per il processo di scansione:

- **Esegui il task di scansione con Bassa Priorità.** Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci ed incrementerai il tempo necessario per finire il processo di scansione.
- **Minimizza la finestra di scansione nel systray.** Riduce a icona la finestra di scansione sulla barra degli strumenti. Eseguire un doppio clic sull'icona di BitDefender per riaprirla.
- **Spegnere il computer quando la scansione sia completata e non siano state rilevate delle minacce**

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Personalizzazione del Livello di Scansione

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Cliccare su **Personalizza** per impostare le vostre opzioni di scansione. Si aprirà una nuova finestra.

Impostazioni di Scansione

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Le opzioni di scansione sono raggruppate in 3 categorie:

- **Livello di Scansione.** Specificare il tipo di malware che volete che Bit Defender analizzi, selezionando le opzioni appropriate dalla categoria **Livello di scansione**.

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansione applicazione	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.

Opzione	Descrizione
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.

- **Opzioni di scansione virus.** Specificare il tipo di oggetti da esaminare (tipi di file, archivi e così via) selezionando opzioni appropriate dalla categoria **Opzioni di scansione virus**.

Opzione		Descrizione
Esamina file	**Tutti i file**	Verranno esaminati tutti i file, indipendentemente dalla loro tipologia.
	Esaminare solo i program file	Per esaminare soltanto i file di programma. Ciò significa solo i file con le seguenti estensioni: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
Esamina i programmi impaccati		Per esaminare i file impaccati.
Esamina gli archivi		Scansiona negli archivi regolari, tipo .zip, .rar, .ace, .iso e altri. Selezionare la casella di controllo **Scansiona programmi di installazione e archivi chm** se si desidera scansionare questo tipo di file. La scansione dei file archiviati incrementa il tempo di scansione e richiede più risorse di sistema. È possibile impostare una dimensione massima di archivi da scansionare in kilobyte (KB) digitando la

Opzione	Descrizione
	dimensione in questo campo **Limite di dimensione degli archivi da scansionare**.
Scansionare gli archivi di e-mail	Per eseguire la scansione all'interno degli archivi di posta.
Esamina settore di boot	Per esaminare i settori di avvio del sistema.
Scansione della memoria	Scansiona la memoria alla ricerca di virus e altro malware.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Scansione di file cookie.

- **Opzioni di azione.** Specificare le azioni da intraprendere per ogni categoria dei file rilevati usando le opzioni in questa categoria.

Nota

Per impostare una nuova azione, fare clic sulla **Prima azione** attuale e selezionare l'opzione desiderata dal menu. Specificare una **Seconda azione** che sarà intrapresa qualora la prima non riuscisse.

▶ Selezionare l'azione da intraprendere sui file infetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

▶ Selezionare l'azione da intraprendere sui file sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file sospetti. Questi file appariranno nel file di report.

Azione	Descrizione
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota

La Scansione euristica ha rilevato dei file sospetti. Vi consigliamo di inviarli al laboratorio di BitDefender.

▶ Selezionare l'azione da intraprendere sugli oggetti nascosti (rootkits) rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.
Muova i files in Quarantena	Sposta i file nascosti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota

Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

▶ **Opzioni per file protetti da password e criptati.** File criptati utilizzando Windows potrebbero essere importanti. Ecco perché è possibile configurare differenti azioni da intraprendere per file infetti o sospetti che sono criptati utilizzarti Windows. Un'altra categoria di file che richiede azioni speciali sono gli archivi protetti da password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Utilizzare queste opzioni per configurare le azioni da intraprendere per archivi protetti da password e per file criptati con Windows.

- **Azione da intraprendere quando viene rilevato un file criptato infetto.** Selezionare l'azione da intraprendere su file infetti criptati usando Windows. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file infetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati. La disinfezione può fallire in alcuni casi, come quando il file infetto è all'interno di specifici archivi di posta.
Cancella i file	Rimuovere immediatamente dal disco i file infetti, senza alcun avviso.
Muova i files in Quarantena	Spostare i file infetti dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- **Azione da intraprendere quando viene rilevato un file criptato sospetto.** Selezionare l'azione da intraprendere su file sospetti criptati usando Windows. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file sospetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- **Azione da intraprendere quando viene rilevato un file protetto da password.** Selezionare l'azione da intraprendere sui file protetti da password rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Registra solo	Tenere registro solo dei file protetti da password nel log di scansione Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Chiedere password	Quando viene rilevato un file protetto da password, chiedere all'utente di fornire la password per poter esaminare il file.

Se clicchi su **Predefinito** verranno applicate le impostazioni di default. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Impostazione del Target di Scansione

Per impostare il target di scansione a una attività di scansione specifica di un utente, fare clic con il pulsante di destra e selezionare **Percorsi**. Alternativamente, se si è già nella finestra Proprietà di un'attività, selezionare la scheda **Percorsi**. Apparirà la finestra seguente:

Target di scansione

Potete vedere la lista di dischi locali, di rete e rimuovibili, ed anche i file e cartelle aggiunti in precedenza, se ci sono. Tutti gli oggetti selezionati verranno esaminati all'esecuzione della funzione.

Sono disponibili i seguenti tasti:

- **Aggiungi Oggetti** - apre una finestra di visualizzazione dove è possibile selezionare i file o le cartelle che si desidera esaminare.

Nota
Utilizzare seleziona & trascina per aggiungere file/cartelle all'elenco.

- **Cancellare Oggetti** - rimuove il (i) file / cartella(e) precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota
Possono essere cancellati solo i file / cartelle aggiunti successivamente e non quelli “visti” automaticamente da BitDefender.

Oltre a questi pulsanti, vi sono altre opzioni che permettono la selezione veloce delle posizioni di scansione.

- **Dischi locali** - per esaminare i drives locali.
- **Dischi di rete** - per esaminare tutti i drive di rete.
- **Drive Rimovibili** - per esaminare i drive rimovibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drive, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

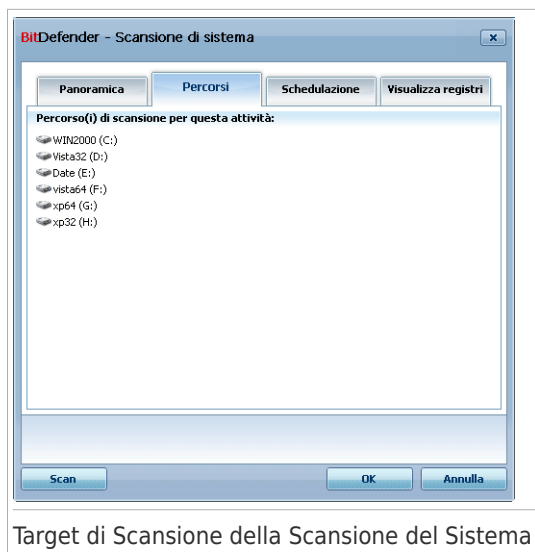
Nota
Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Visualizzazione del Target di Scansione delle Funzioni del Sistema

Non è possibile modificare il target di scansione delle attività di scansione dalla categoria **Attività di Sistema**. Potete solo visualizzare il loro target di scansione.

Per visualizzare il target di scansione di una specifica attività di scansione del sistema, fare clic con il tasto destro sull'attività e selezionare **Mostra Percorsi di Scansione**. Per **Scansione del sistema**, ad esempio, apparirà la seguente finestra:

Target di Scansione della Scansione del Sistema

Scansione del sistema e **Scansione approfondita del sistema** scansioneranno tutti i drive locali, mentre **Scansione veloce del sistema** scansionerà solo le cartelle `Windows` e `Program Files`.

Selezionare **OK** per chiudere la finestra. Per eseguire la funzione, cliccare semplicemente **eseguire scansione**.

Programmazione delle Funzioni di Scansione

Una scansione completa può richiedere un certo tempo e agisce meglio se vengono chiusi tutti gli altri programmi. La miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene utilizzato.

Per vedere il programma di un'attività specifica o per modificarlo, fare clic con il pulsante destro sull'attività e selezionare **Programmazione**. Se si è già nella finestra Proprietà dell'attività, selezionare la scheda **Utilità di pianificazione**. Apparirà la finestra seguente:

Schedulazione

Potete vedere la programmazione delle funzioni, se ci sono.

Quando programmate un compito, dovete scegliere una delle seguenti opzioni:

- **No** - lancia la scansione solo quando richiesta dall'utente.
- **Una volta** - lancia la scansione solo una volta, in un certo momento. Specificare la data e l'ora di avvio nel campo **Start Date/Time**.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (minuti, ore, giorni, settimane, mesi) iniziando da una certa data ed ora specificate.

  Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo **Ogni** il numero di minuti / ore / giorni / settimane / mesi indicando la frequenza del processo. È inoltre necessario specificare la data e l'ora di inizio nei campi **Data/Ora di inizio**.
- **All'avvio del sistema** - lancia la scansione un numero specifico di minuti dopo che l'utente ha effettuato l'accesso a Windows.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

18.2.5. Scansione file e cartelle

Prima di iniziare il processo di scansione, assicurarsi che BitDefender sia aggiornato con le firme malware. Eseguire la scansione usando un database delle impronte obsoleto può impedire BitDefender di rilevare nuovo malware, trovato dopo l'ultimo

aggiornamento. Per verificare quando è stato eseguito l'ultimo aggiornamento, fare clic su **Aggiornamento>Aggiornamento** in Visualizzazione avanzata.

Nota
Per consentire a BitDefender di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. E’ soprattutto importante chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Consiglio di scansione

Ecco altri consigli sulla scansione che potrebbero essere utili:

- In base alla dimensione del disco rigido, l'esecuzione di una scansione comprensiva del computer (ad esempio una Scansione approfondita del sistema o una Scansione del sistema) potrebbe richiedere molto tempo (fino ad un ora o più). Quindi, si dovrebbero eseguire tali scansioni quando non si usa il computer per un lungo periodo di tempo (ad esempio di notte).

  È possibile programmare la scansione affinché inizi quando è più conveniente. Assicurarsi di lasciare il computer accesso. Con Windows Vista, assicurarsi che il computer non sia nella modalità sospensione quando l'attività deve essere eseguita.
- Se si scaricano spesso file da Internet ad una cartekka specifica, si consiglia di creare una nuova attività di scansione e impostare quella cartella come target della scansione. Programmare l'attività affinché venga eseguita una volta al giorno o più spesso.
- Esiste un malware che si imposta per essere eseguito ad ogni avvio del sistema modificando le impostazioni di Windows. Per proteggere il computer da un tale malware, è possibile programmare che l'attività **Scansioen accesso automatico** venga eseguito all'avvio del sistema. Notare che la scansione accesso automatico potrebbe influenzare la performance del sistema per un breve periodo di tempo dopo l'avvio.

Metodi di Scansione

BitDefender consente quattro tipi di scansione a richiesta:

- Scansione immediata - avvia immediatamente un processo di scansione dal sistema / funzioni utente.
- Scansione contestuale - fare clic con il pulsante destro su un file o una cartella e selezionare **Scansione con BitDefender**.
- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione.
- Scansione manuale - Utilizzare Scansione Manuale di BitDefender per selezionare direttamente i file o cartella da esaminare.

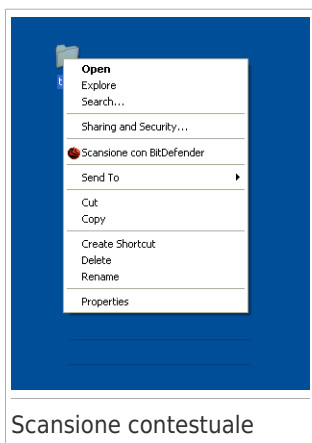
Scansione Immediata

Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default oppure i vostri propri compiti di scansione. Ciò si chiama scansione immediata

Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Contestuale

Per esaminare un file o cartella senza configurare un nuovo compito di scansione, si può usare il menu contestuale. ciò si chiama scansione contestuale

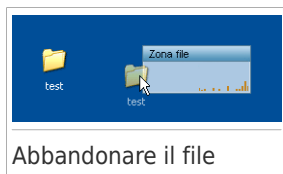
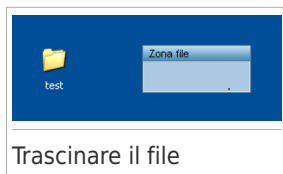
Scansione contestuale

Fare clic con il pulsante destro del mouse sul file o la cartella che si desidera scansionare e selezionare **Scansiona con BitDefender**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

E' possibile modificare e vedere il file di report dalla finestra delle **Proprietà** del **Menu Scansione Contestuale**.

Scansione Seleziona e Trascina

Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file

Abbandonare il file

La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Manuale

La scansione manuale consiste in selezionare direttamente l'oggetto da esaminare, utilizzando l'opzione Scansione Manuale BitDefender dal gruppo di programmi BitDefender nel Menu di Avvio.

Nota
La scansione manuale è molto utile, poichè può essere eseguita anche quando Windows lavora in Modalità Provvisoria.

Per selezionare l'oggetto da scansionare con BitDefender, nel menu Avvio di Windows, seguire il percorso **Avvio** → **Programmi** → **BitDefender 2010** → **Scansione Manuale di BitDefender**. Apparirà la finestra seguente:

Scansione Manuale

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

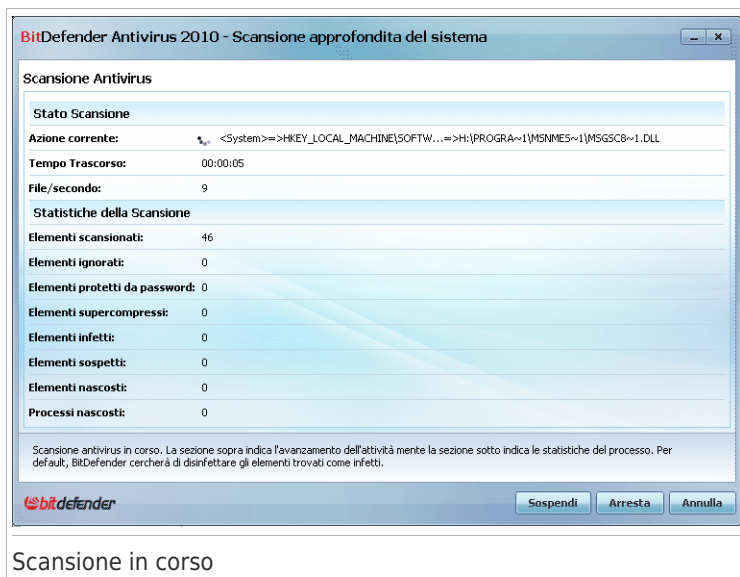
Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Procedura guidata scansione antivirus

Quando si avvia la scansione su richiesta, apparirà la Procedura guidata Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che BitDefender finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se BitDefender rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Password.** Se si desidera che BitDefender scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non chiedere una password e ignorare questo oggetto durante la scansione.** Selezionare questa opzione per non scansionare questo archivio.
- **Ignora tutti gli elementi protetti da password senza scansionarli.** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli

archivi protetti da password. BitDefender non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

Riassunto

E’ possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante

Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

BitDefender potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.it. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

BitDefender ha rilevato dei file sospetti.

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab BitDefender. Cliccare su **OK** per inviare questi file ai laboratori BitDefender per ulteriori analisi.

18.2.6. Visualizzazione dei Registri di Scansione

Per visualizzare i risultati della scansione una volta completata un'attività, fare clic con il tasto destro sull'attività e selezionare **Visualizza Registri**. Apparirà la finestra seguente:

Esaminare registri

Qui potete trovare i file del report generati ogni che una funzione viene eseguita. In ogni file vengono fornite informazioni sullo stato del processo di scansione registrato, la data e l'ora in cui la scansione è stata eseguita ed un riassunto sui risultati della scansione.

Sono disponibili due pulsanti:

- **Cancellare** - per eliminare il log di scansione selezionato.
- **Mostrare** - per visualizzare il log di scansione selezionato. Il registro di scansione si aprirà nel vostro web browser predefinito.

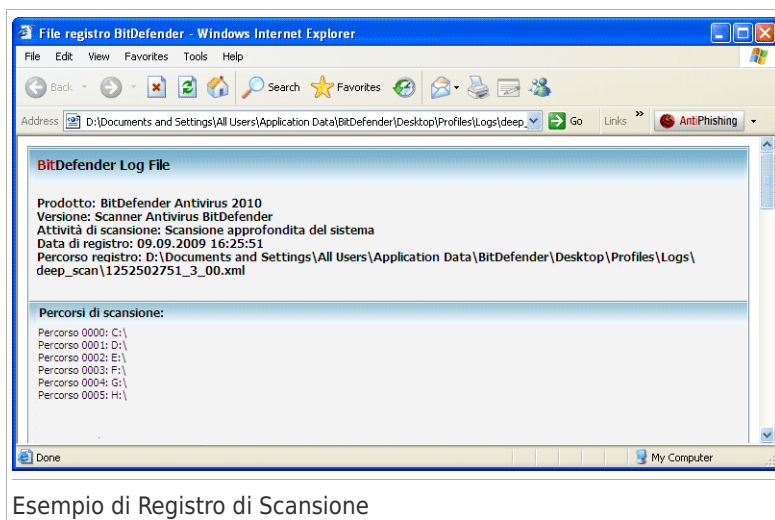
Nota

Inoltre, per visualizzare o cancellare un file, fare clic con il pulsante destro sul file e selezionare l'opzione corrispondente dal menu di scelta rapida.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Esempio di Registro di Scansione

La seguente figura rappresenta un esempio di registro di scansione:

Esempio di Registro di Scansione

Il log di scansione contiene informazioni dettagliate sul processo di scansione registrato, sul target di scansione, le minacce individuate e le azioni intraprese su queste minacce.

18.3. Oggetti esclusi dalla scansione

Ci sono dei casi in cui si può avere bisogno di escludere certi file dalla scansione. Ad esempio, si può volere escludere un file di testo EISCAR dalla scansione all'accesso, oppure i file `.avi` dalla scansione a richiesta.

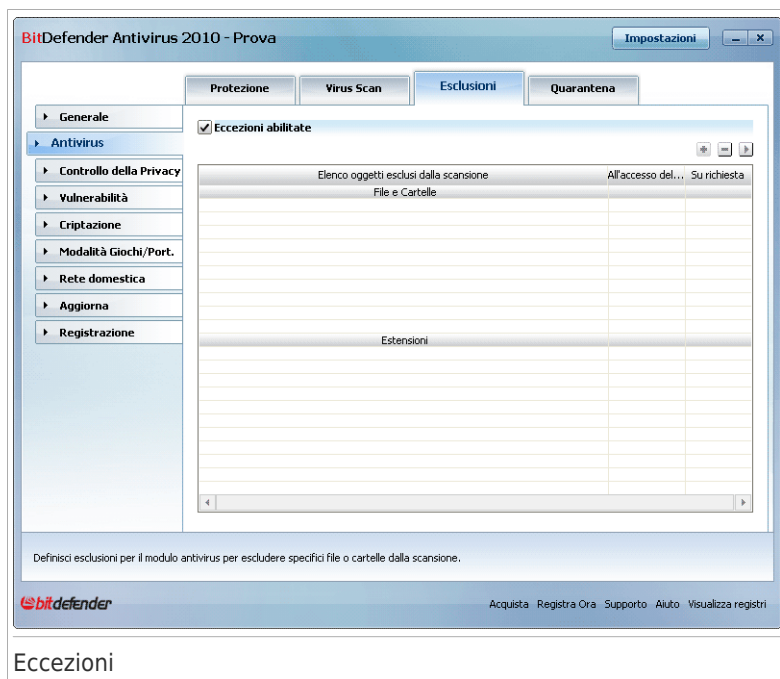
BitDefender permette di escludere oggetti dalle scansioni all'accesso ed a richiesta, o da entrambi. Questa caratteristica cerca di ridurre i tempi di scansione e di evitare le interferenze con il vostro lavoro.

Due tipi di oggetti possono essere esclusi dalla scansione:

- **Percorsi** - Il file o cartella (inclusi tutti gli oggetti che essi contiene) indicato da un percorso specifico verrà escluso dalla scansione.
- **Estensioni** - tutti i file che hanno una specifica estensione verranno esclusi dalla scansione.

Nota

Gli oggetti esclusi dalla scansione all'accesso non verranno esaminati, non importa se sono visitati da voi o da un'applicazione.

Per visualizzare e gestire gli oggetti esclusi dalla scansione, fare clic su **Antivirus>Eccezioni** in Modalità Avanzata.

Eccezioni

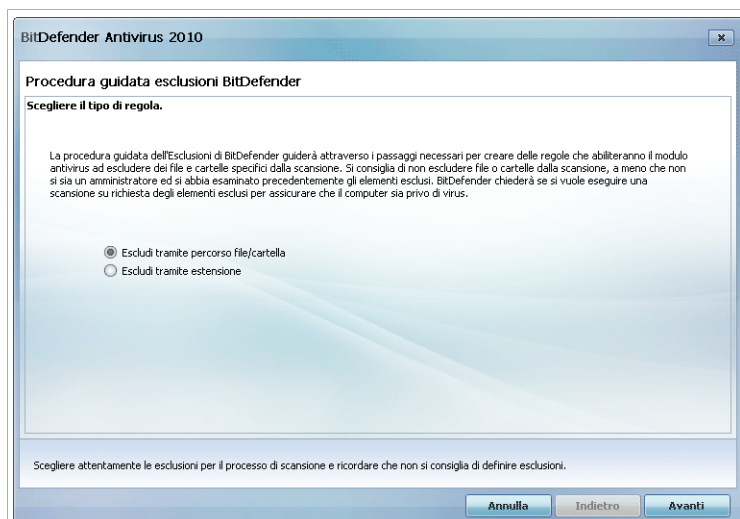
Si possono visualizzare gli oggetti (file, cartelle, estensioni) esclusi dalla scansione. Potete vedere se ogni oggetto è stato escluso dalla scansione all'accesso, dalla scansione a richiesta o da entrambi.

Nota

Le eccezioni qui specificate NON verranno applicate nella scansione contestuale. La scansione contestuale è un tipo di scansione su richiesta: fare clic con il pulsante destro sul file o cartella che si vuole scansionare e selezionare **Scansiona con BitDefender**.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una voce dalla tabella, selezionarla e fare clic sul pulsante **Modifica**. Apparirà una nuova finestra dove si potrà modificare l'estensione od il percorso da

escludere ed il tipo di scansione dal quale escluderlo, a seconda delle necessità. Apportare le necessarie modifiche e cliccare **OK**.

Nota
È inoltre possibile fare clic con il pulsante destro sull'oggetto ed utilizzare le opzioni del menu di scelta rapida per modificarlo o eliminarlo.

Potete cliccare su **Ignorare** per ritornare alla situazione precedente alle modifiche effettuate alla tabella delle regole, sempre che non le abbiate salvate cliccando su **Applicare**.

18.3.1. Esclusione dei Percorsi dalla Scansione

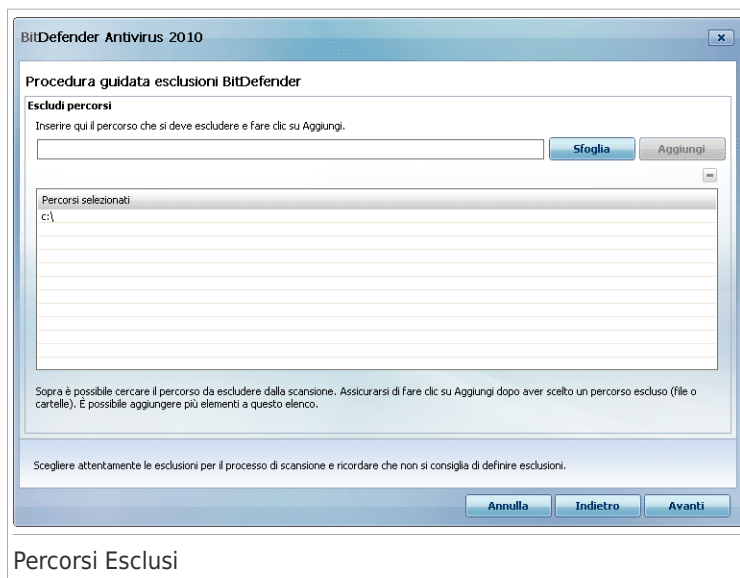
Per escludere dei percorsi dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione dei percorsi dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare i percorsi esclusi

Percorsi Esclusi

Per specificare i percorsi da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Cliccare **Sfoglia**, selezionare il file o cartella che volete venga escluso dalla scansione e quindi cliccare su **Aggiungere**.
- Scrivere il percorso che volete venga escluso dalla scansione nel campo modifica e cliccare **Aggiungere**.

Nota
Se il percorso inserito non esiste, comparirà un messaggio di errore. Cliccare **OK** e controllare la validità del percorso.

I percorsi appariranno nella tabella man mano che vengono aggiunti. Potete aggiungere quanti percorsi volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Selezionare **Avanti**.

Passo 3/4 – Selezionare tipo di scansione

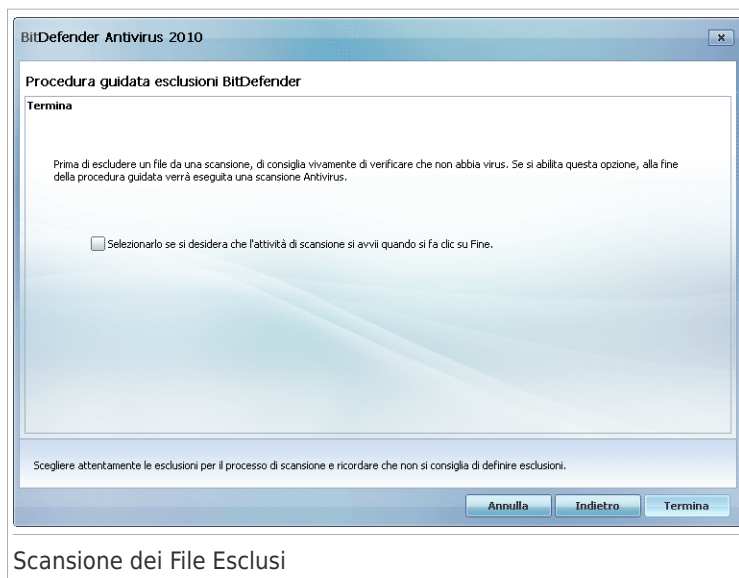
Tipo di Scansione

Potete vedere una tabella contenente i percorsi da escludere dalla scansione ed il tipo di scansione dal quale vengono esclusi.

Per default i percorsi selezionati verranno esclusi da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

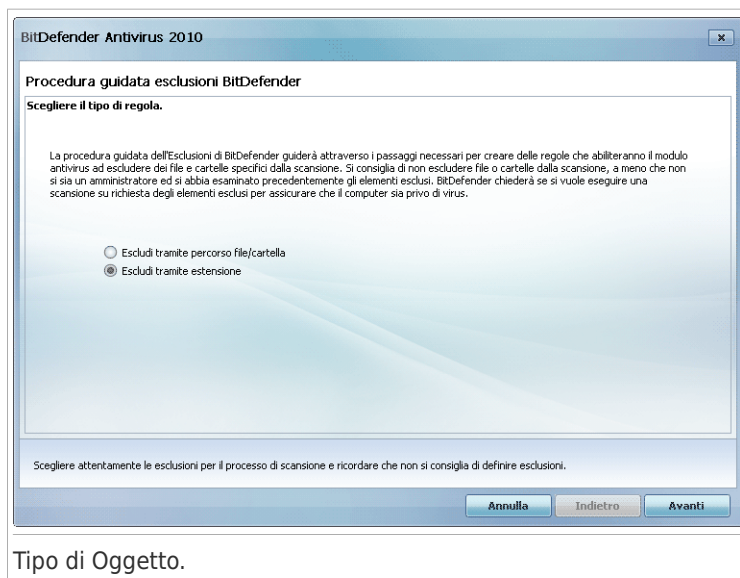
Passo 4/4 – Esaminare i file esclusi

Scansione dei File Esclusi

E' altamente consigliato esaminare i file nei percorsi specificati per essere sicuri che non siano infetti. Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Termina**.

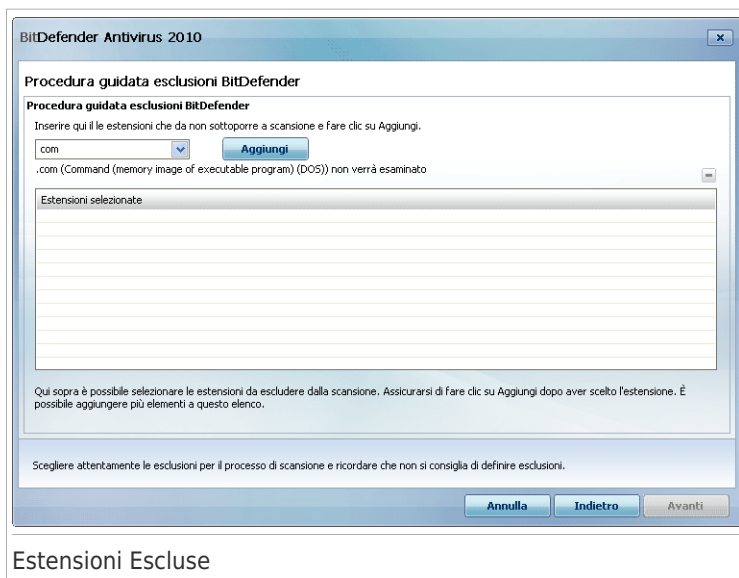
18.3.2. Esclusione delle Estensioni dalla Scansione

Per escludere delle estensioni dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione delle estensioni dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere estensioni dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare le estensioni escluse

Estensioni Escluse

Per specificare le estensioni da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Selezionare dal menu l'estensione che volete venga esclusa dalla scansione e quindi cliccare su **Aggiungere**.

Nota
Il menu contiene un elenco di tutte le estensioni registrate sul vostro sistema. Quando selezionate un'estensione, potrete vedere la sua descrizione, se disponibile.

- Scrivere l'estensione che volete venga esclusa dalla scansione nel campo modifica e cliccare **Aggiungere**.

Le estensioni appariranno nella tabella man mano che vengono aggiunte. Potete aggiungere quante estensioni volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Selezionare **Avanti**.

Passo 3/4 – Selezionare tipo di scansione

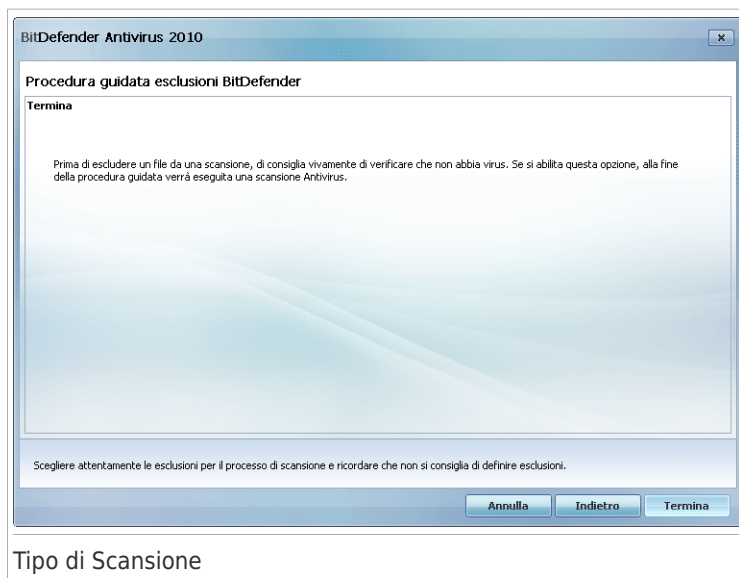
Tipo di Scansione

Potete vedere una tabella contenente le estensioni da escludere dalla scansione ed il tipo di scansione dal quale vengono escluse.

Per default le estensioni selezionate verranno escluse da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

Passo 4/4 – Selezionare tipo di scansione

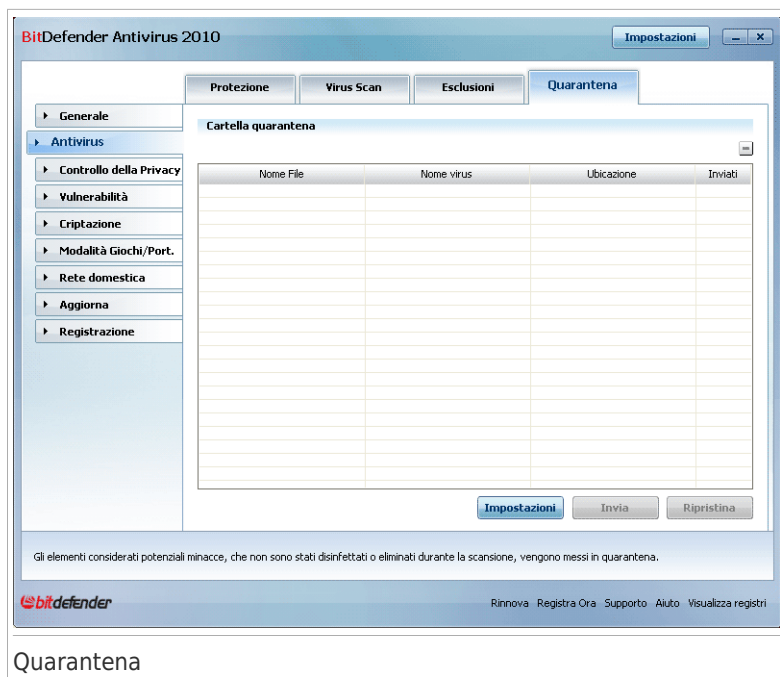
Tipo di Scansione

E' altamente consigliato esaminare i file con le estensioni specificate per essere sicuri che non siano infetti.

Selezionare **Termina**.

18.4. Area di Quarantena

BitDefender consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi file in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi file ai Laboratori BitDefender per ulteriori analisi.

Inoltre BitDefender scansiona i file in quarantena dopo ogni aggiornamento di firme malware. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per visualizzare e gestire i file in quarantena e per configurare le impostazioni della quarantena, fare clic su **Antivirus>Quarantena** in Modalità Avanzata.

Quarantena

La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena. Per ogni file in quarantena, potete vedere il suo nome, il nome del virus rilevato, il percorso alla sua posizione originale e la data di invio.

Nota

Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

18.4.1. Gestione dei File in Quarantena

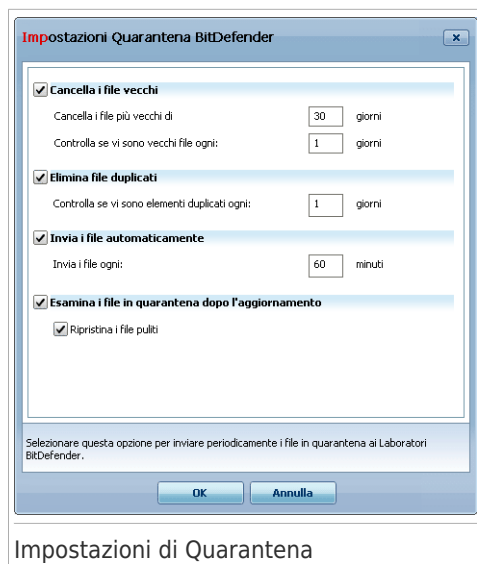
Potete inviare qualsiasi file selzionato dalla quarantena al lab BitDefender cliccando su **Invia**. Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

Per cancellare un file selezionato dalla quarantena, fare clic sul pulsante **Elimina**. Se si desidera inviare un file selezionato alla sua ubicazione originale, fare clic su **Riprisitina**.

Menù contestuale. E' disponibile un menu contestuale che vi permette di gestire facilmente i file in quarantena. Sono disponibili le stesse opzioni su menzionate. Potete anche selezionare **Aggiornare** per aggiornare la sezione di Quarantena.

18.4.2. Configurazione delle Impostazioni di Quarantena

Per configurare le impostazioni di quarantena, cliccare su **Impostazioni**. Apparirà una nuova finestra.

Impostazioni di Quarantena

Utilizzando le impostazioni di quarantena, potete configurare BitDefender per eseguire automaticamente le seguenti azioni:

Eliminare i vecchi file. Per eliminare automaticamente i vecchi file, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni dopo i quali i file in quarantena devono essere eliminati e la frequenza con cui BitDefender deve effettuare il controllo dei vecchi file.

Nota
Per default, BitDefender effettuerà il controllo dei vecchi file ogni giorno ed eliminerà i file più vecchi di 30 giorni.

Elimina file duplicati. Per eliminare automaticamente i file duplicati in quarantena, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni tra due controlli consecutivi dei duplicati.

Nota
Per default, BitDefender effettuerà il controllo dei file duplicati in quarantena ogni giorno.

Invio automatico dei file. Per inviare automaticamente i file in quarantena, selezionare l'opzione corrispondente. Dovete specificare la frequenza con cui inviare i file.

Nota

Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

Esaminare i file in quarantena dopo l'aggiornamento. Per esaminare automaticamente i file in quarantena dopo l'aggiornamento, selezionare l'opzione corrispondente. Potete scegliere di far tornare automaticamente i file puliti alla loro posizione originale selezionando **Ripristinare file puliti**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

19. Controllo della Privacy

BitDefender esegue il monitoraggio di dozzine di potenziali “hotspots” nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.

19.1. Statistiche Controllo Privacy

Per configurare il Controllo della Privacy e visualizzare informazioni riguardanti la sua attività, andare su **Controllo della Privacy>Stato** in Modalità Avanzata.

Statistiche Controllo Privacy

Potete vedere se il Controllo della Privacy è abilitato o disabilitato. Se desiderate cambiare lo stato del Controllo della Privacy, deselezionare o selezionare la casella corrispondente.

Importante

Per evitare il furto e proteggere la vostra privacy, mantenere il **Controllo della Privacy** attivo.

Il Controllo della Privacy protegge il vostro computer utilizzando questi importanti controlli di protezione:

- Controllo Identità - protegge i vostri dati riservati filtrando tutto il traffico web (HTTP), mail (SMTP), e chat in uscita secondo le regole da voi create nella sezione Identità.
- Controllo di Registro - chiede il vostro permesso ogni volta che un programma cerca di modificare una chiave di registro per essere eseguita all'avvio di Windows.
- Controllo dei Cookie - chiederà il vostro consenso ogni volta che un sito web tenterà di impostare un cookie.
- Controllo degli Script - chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o un altro contenuto attivo.

Nel lato inferiore della sezione è possibile vedere le **Statistiche Controllo della Privacy**.

19.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Tutti i controlli di protezione sono disabilitati.
Default	Solo il **Controllo di Identità** è abilitato.
Aggressiva	**Controllo Identità**, **Controllo Registro**, **Controllo Cookie** e **Controllo Script** sono abilitati.

E' possibile personalizzare il livello di protezione cliccando **Livello Personalizzato**. Nella finestra che apparirà, selezionare i controlli di protezione che volete abilitare e cliccare su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

19.2. Controllo Identità

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. I furto di dati ha tenuto il passo con lo siluppo delle comunicazioni via Internet e fa

uso di nuovi metodi per ingannare le persone inducendole a dare via informazioni private.

Che sia la vostra e-mail o il numero della vostra carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarvi danno: potete trovarvi affogati nei messaggi di spam o potreste essere sorpresi nell'accedere ad un conto svuotato.

Il Controllo Identità vi protegge dal furto di dati sensibili quando siete online. Basandosi sulle regole create da voi, il Controllo Identità esegue la scansione del traffico web, mail ed instant messaging in uscita dal vostro computer, cercando specifiche sequenze di caratteri (ad esempio, la vostra carta d'identità). Se c'è una coincidenza, la pagina web, la mail o il messaggio instantaneo vengono bloccati.

Potete creare regole per proteggere ogni informazione che considerate personale o confidenziale, dal vostro numero di telefono o il vostro inidrizzo mail alle informazioni sul vostro conto in banca. Viene fornito un supporto Multi-utente, in modo che gli utenti che accedano ad altri account di Windows possano configurare ed usare le proprie regole di protezione dell'identità. Se il proprio account Windows è un account amministratore, le regole create possono essere configurate per essere applicate anche quando altri utenti del computer accedono ai rispettivi account utente Windows.

Perché usare il Controllo Identità?

- Il controllo identità è molto efficace nel bloccare lo spyware keylogger. Questo tipo di applicazione maligna registra le vostre battute sulla tastiera e le invia tramite Internet ad un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come i numeri e password di un conto corrente, ed usarle per ottenere benefici personali.

  Supponendo che tale applicazione riesca ad evitare la rilevazione antivirus, non potrà inviare i dati rubati via e-mail, web o chat se avete creato regole appropriate per la protezione dell'identità.

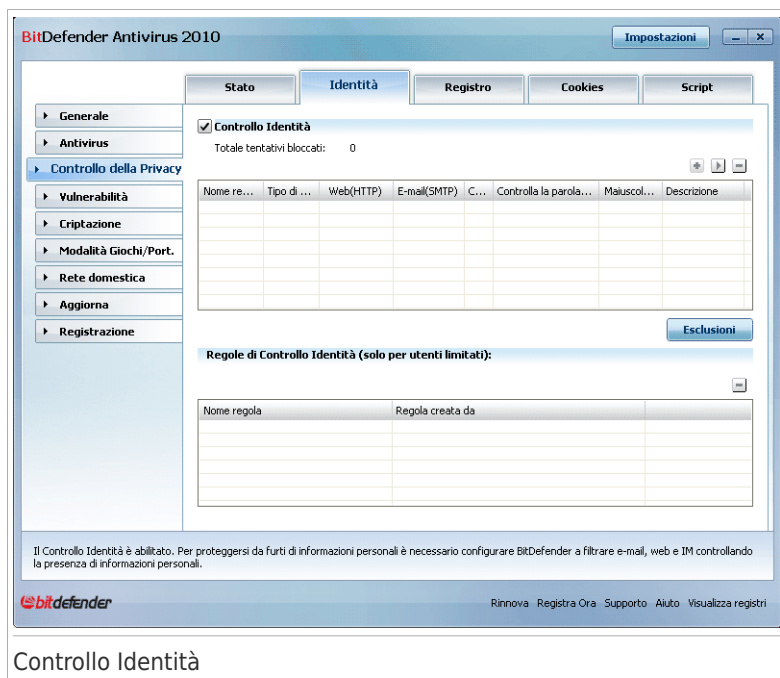
- Il Controllo identità vi può proteggere dai tentativi di phishing (tentativi di rubare informazioni personali). I tentativi più comuni di phishing fanno uso di e-mail ingannevoli per convincervi ad inviare informazioni personali ad una falsa pagina web.

  Ad esempio, potreste ricevere una mail che si proclama venire dalla vostra banca e vi richiede di aggiornare urgentemente le informazioni sul vostro conto. La mail vi fornisce un link alla pagina web dove dovreste inserire vostre informazioni personali. Anche se sembrano legittime, le mail e le pagine web alle quali vi conduce il falso link sono fasulle. Se cliccate sul link nella mail ed inviate le vostre informazioni personali alla falsa pagina web, svelerete queste informazioni alle persone che hanno organizzato il tentativo di phishing.

  Se ci sono le appropriate regole di protezione dell'identità, non potrete inviare informazioni personali (come il numero della vostra carta di credito) ad una pagina

web, a meno che non abbiate esplicitamente definito un'eccezione per questa pagina.

Per configurare il Controllo Identità, fare clic su **Controllo della Privacy>Identità** in Modalità avanzata.

Controllo Identità

Se volete usare il Controllo Identità, seguire questi passi:

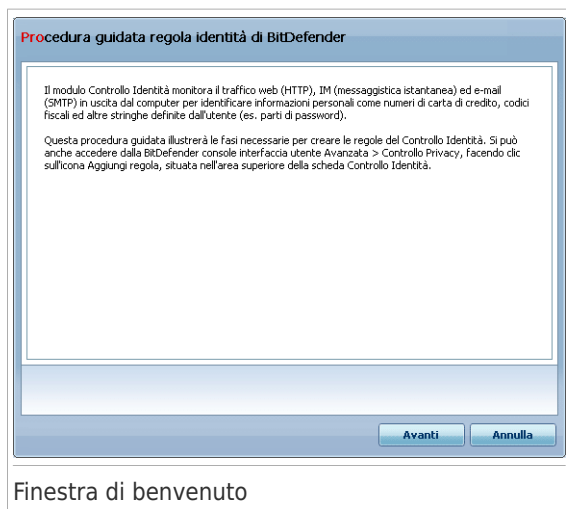
1. Selezionare la casella di controllo **Abilita controllo Identità**.
2. Creare regole per proteggere i vostri dati sensibili. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Creazione delle Regole d'Identità»* (p. 156).
3. Se necessario, definire esclusioni specifiche alle regole create. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Definizione Esclusioni»* (p. 159).
4. Se si è un amministratore del computer, è possibile escludere se stessi dalle regole di identità create da altri amministratori.

   Per ulteriori informazioni, fare riferimento a *«Regole definite da altri amministratori»* (p. 161).

19.2.1. Creazione delle Regole d'Identità

Per creare una regola di protezione dell'identità, fare clic sul pulsante **Aggiungi** e seguire procedura guidata di configurazione.

Passo 1/4 - Finestra di Benvenuto

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/4 - Impostazione Tipo di Regola e Dati

Impostare il Tipo di Regola e i Dati

Dovete impostare i parametri seguenti:

- **Nome Regola** - inserire il nome della regola nel campo di modifica.
- **Tipo di Regola** - scegliere il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN etc).
- **Dati Regola** - inserire i dati da proteggere nel campo di modifica. Ad esempio, se si vuole proteggere la carta di credito, inserire tutto o parte del numero in questo campo.

Nota
Se inserite meno di tre caratteri, vi verrà chiesto di validare i dati. Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

Tutti i dati che inserite sono criptati. Per una sicurezza maggiore, non inserire tutti i dati che volete proteggere.

Selezionare **Avanti**.

Passo 3/4 - Selezionare i Tipi di Traffico e gli Utenti

Selezionare i Tipi di Traffico e gli Utenti

Selezionare il traffico che si desidera esaminare con BitDefender. Sono disponibili le seguenti opzioni:

- **Scansione web (traffico HTTP)** - scansiona il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
- **Scansione e-mail (traffico SMTP)** - esamina il traffico SMTP (mail) e blocca le mail in uscita contenenti i dati della regola.
- **Scansione IM (Instant Messaging)** - scansiona il traffico Instant Messaging e blocca i messaggi in uscita contenenti i dati della regola.

Potete scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

Specificare gli utenti a cui si applica la regola.

- **Solo per me (utente attuale)** - la regola si applica solo all'account utente attuale.
- **Account utente limitati** - la regola si applica all'utente attuale e a tutti gli account di Windows limitati.
- **Tutti gli utenti** - la regola si applica a tutti gli account di Windows.

Selezionare **Avanti**.

Passo 4/4 – Descrizione Regola

Definizione Regola

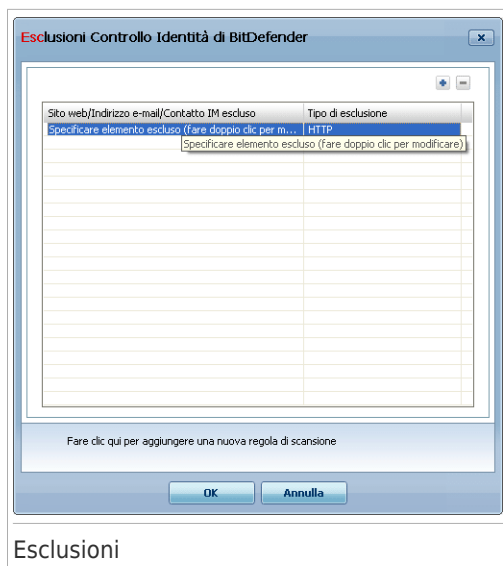
Inserire una breve descrizione della regola nel campo di editing. Siccome i dati bloccati (serie di caratteri) non vengono mostrati in plain text quando si accede alla regola, la descrizione dovrebbe aiutarvi ad identificarla facilmente.

Selezionare **Termina**. La regola apparirà nella tabella.

19.2.2. Definizione Esclusioni

Ci sono dei casi in cui dovrete definire eccezioni a specifiche regole d'identità. Consideriamo il caso in cui voi create una regola che impedisca l'invio attraverso HTTP (web) del numero della vostra carta di credito. Ogni volta che il numero della vostra carta di credito verrà inviato ad un sito web dal vostro account, la rispettiva pagina verrà bloccata. Se volete, per esempio, comprare delle scarpe in un negozio on line (che sapete che è sicuro), dovrete specificare un'eccezione alla rispettiva regola.

Per aprire la finestra dove si possono gestire le eccezioni, fare clic su **Esclusioni**.

Esclusioni

Per aggiungere un'eccezione, seguire i seguenti passi:

1. Selezionare **Aggiungi** per aggiungere una nuova regola alla tabella.
2. Fare doppio clic su **Specifica elementi esclusi** e fornire gli indirizzi web, mail o chat che si desidera vengano aggiunti come eccezione.
3. Fare clic due volte su **Tipo traffico** e scegliere dal menu l'opzione corrispondente al tipo d'indirizzo fornito in precedenza.
   - Se avete scelto un indirizzo web, selezionare **HTTP**.
   - Se avete specificato un indirizzo mail, selezionare **E-mail (SMTP)**.
   - Se avete specificato un contatto chat, selezionare **Chat**.

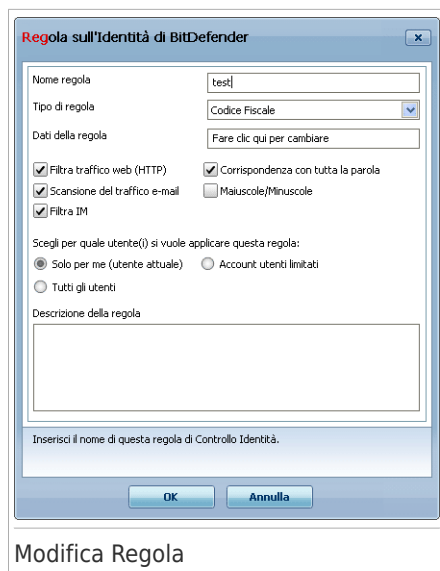
Per rimuovere un'eccezione dall'elenco, selezionarla e fare clic sul pulsante **Rimuovi**.

Selezionare **Applica** per salvare le modifiche.

19.2.3. Amministrazione delle regole

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** oppure fare doppio clic su di essa. Apparirà una nuova finestra.

Modifica Regola

Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Cliccate su **OK** per salvare le modifiche.

19.2.4. Regole definite da altri amministratori

Se non si è l'unico utente con diritti di amministratore sul sistema, gli altri amministratori possono creare regole di identità a proprio piacimento. Nel caso si desideri che le regole create da altri utenti non si applichino quando si è effettuato l'accesso, BitDefender permette di escludere se stessi da qualsiasi regola che non si sia creata.

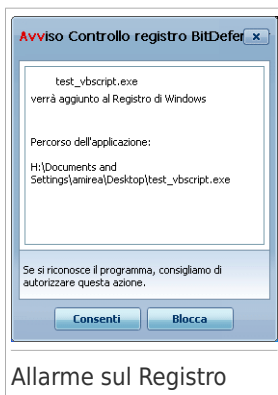
È possibile vedere un elenco di regole create da altri amministratori nella tabella sotto la voce **Regole di controllo Identità**. Per ogni regola viene elencato il nome e l'utente che l'ha creata.

Per escludersi da una regola, selezionarla nella tabella e fare clic sul pulsante **Elimina**.

19.3. Controllo dei Registri

Una componente molto importante del sistema operativo di Windows si chiama **Registro**. E’ dove Windows tiene le informazioni relative alle proprio configurazioni, ai programmi installati, all’utente e così via.

Il **Registro** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo dei Registri** sorveglia il Registro di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registro per poter essere eseguito all'avvio di Windows.

Allarme sul Registro

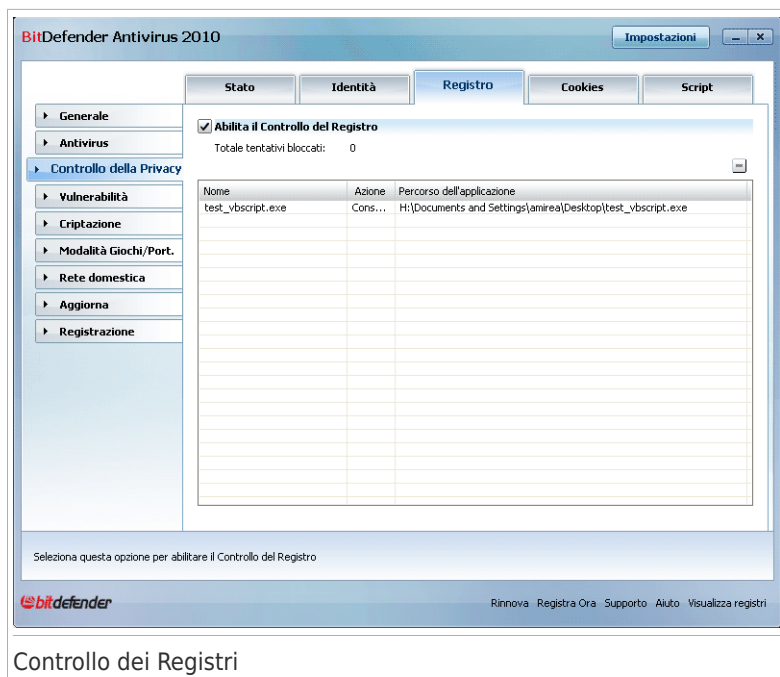
Potete vedere il programma che sta tentando di modificare il Registro di Windows.

Se non riconoscete il programma e vi sembra sospetto, cliccare su **Bloccare** per impedirgli di modificare il Registro di Windows. Altrimenti, cliccare su **Consentire** per permettere la modifica.

In base alla vostra risposta, viene creata una regola e viene elencata nella tabella delle regole. La stessa azione viene applicata ogni volta che questo programma tenta di modificare una chiave di registro.

Nota

BitDefender vi avviserà, di norma, quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Per configurare il Controllo di Registro, andare a **Controllo della Privacy>Registro** in Modalità Avanzata.

Controllo dei Registri

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

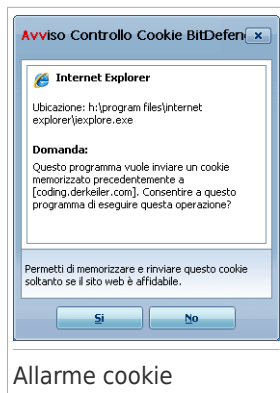
19.4. Controllo dei Cookie

I cookie sono molti frequenti su Internet. Si tratta di piccoli file immagazzinati sul vostro computer. I siti web creano questi cookie per tenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookie vengono creati per rendere facilitare le cose. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, così da non doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra riservatezza, tenendo traccia delle vostre abitudini di navigazione.

E’ qui che il **Controllo dei Cookie** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookie** chiederà il vostro permesso ogni volta che un sito web tenta di impostare un cookie:

Allarme cookie

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare il file cookie.

Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Ciò aiuterà a scegliere i siti web di cui ci si fida e quelli di cui non ci si fida.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookie** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookie sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

Per configurare il Controllo dei Cookie, fare clic su **Controllo della Privacy>Cookie** in Modalità Avanzata.

Controllo dei Cookie

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per aggiungere manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

19.4.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.

Seleziona Indirizzo, Azione e Direzione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	I cookie da quel dominio verranno eseguiti.
Impedisci	I cookie da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Direzione	Descrizione
In Uscita	La regola verrà applicata solo per i cookie che vengono rispediti al sito connesso.
In Entrata	La regola verrà applicata solo per i cookie che vengono ricevuti dal sito connesso.
Entrambe	La regola sarà applicata in entrambe le direzioni.

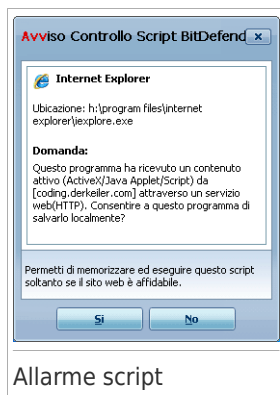
Nota
Si possono accettare i cookie, ma non conviene mai rispedirli, cioè impostando l'azioneo **Divieto** e la direzione **Uscente**.

Selezionare **Termina**.

19.5. Controllo script

Gli Scripts e altri codici come ActiveX controls e Java applets, che sono utilizzati per creare pagine interattive, possono essere programmati per avere effetti dannosi. Per esempio gli elementi ActiveX , possono ottenere l' accesso ai dati del vostro computer, cancellare informazioni, catturare passwords e intercettare messaggi mentre siete online. Dovreste accettare contenuti attivi esclusivamente da siti che si conoscono come affidabili.

BitDefender vi consente di scegliere se eseguire questi elementi o bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete coinvolti nel decidere di quali siti web vi fidate e di quali non vi fidate. BitDefender chiederà il vostro permesso ogni volta che un sito web tenta di attivare uno script o altri contenuti attivi:

Allarme script

E' possibile visualizzare il nome della risorsa.

Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Per configurare il Controllo degli Script, fare clic su **Controllo della Privacy>Script** in Modalità Avanzata.

Controllo script

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per creare manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

19.5.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.

Selezionare Indirizzo ed Azione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	Gli script da quel dominio verranno eseguiti.
Impedisci	Gli script da quel dominio non verranno eseguiti.

Selezionare **Termina**.

20. Vulnerabilità

Un passaggio importante nella protezione del vostro computer contro hackers e applicazioni maligne è mantenere aggiornato il sistema operativo e le applicazioni che usate regolarmente. Inoltre, per impedire accessi fisici non autorizzati al vostro computer, dovete configurare password forti (password che non possano essere facilmente indovinate) per ogni account di Windows.

BitDefender controlla regolarmente il vostro sistema alla ricerca di vulnerabilità e vi avverte dei problemi esistenti.

20.1. Stato

Per configurare il controllo automatico delle vulnerabilità o per eseguire un controllo delle vulnerabilità, fare clic su **Vulnerabilità>Stato** in Modalità Avanzata.

Stato Vulnerabilità

La tabella mostra i problemi trovati nell'ultima scansione delle vulnerabilità e il loro stato. Potete vedere l'azione intrapresa per riparare le vulnerabilità, se necessario. Se l'azione **negativa** allora il rispettivo problema non rappresenta una vulnerabilità.

Importante

Per essere avvertiti automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantenere il **Controllo Automatico delle Vulnerabilità** abilitato.

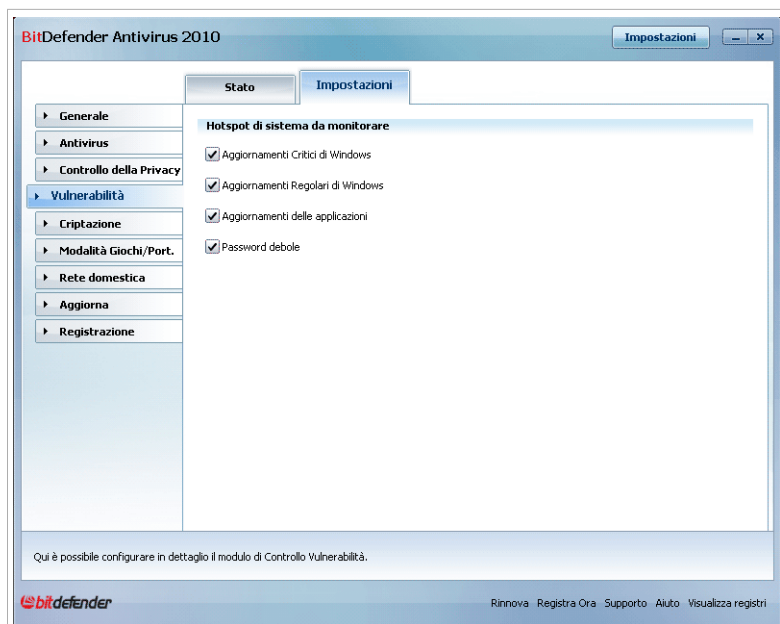
20.1.1. Correggi Vulnerabilità

A seconda del problema, per risolvere una vulnerabilità specifica procedere come segue:

- Se sono disponibili aggiornamenti di Windows, fare clic su **Installa** nella colonna **Azione** per installarli.
- Se un'applicazione non è aggiornata, cliccare sul link fornito **Home Page** per scaricare la versione più recente.
- Se un account utente Windows ha una password debole, fare clic su **Risolvi** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiate voi stessi la password. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Per controllare le possibili vulnerabilità del vostro computer, clicca su **Controlla adesso** e seguire la procedura guidata. Per ulteriori informazioni fare riferimento a *«Procedura guidata di Controllo delle vulnerabilità»* (p. 65).

20.2. Impostazioni

Per configurare le impostazioni del controllo automatico delle vulnerabilità andare su **Vulnerabilità>Impostazioni** in Modalità Avanzata.

Impostazioni del Controllo Automatico delle Vulnerabilità

Selezionare le caselle corrispondenti alle vulnerabilità del sistema che volete vengano controllate regolarmente.

- **Aggiornamenti Critici di Windows**
- **Aggiornamenti Regolari di Windows**
- **Aggiornamenti applicazioni**
- **Password Deboli**

Nota

Se deselezionate la casella corrispondente ad una vulnerabilità specifica, BitDefender non vi avvertirà più sui relativi problemi.

21. Criptazione Chat (IM)

Di default, BitDefender esegue la criptazione di tutte le vostre sessioni chat, purché:

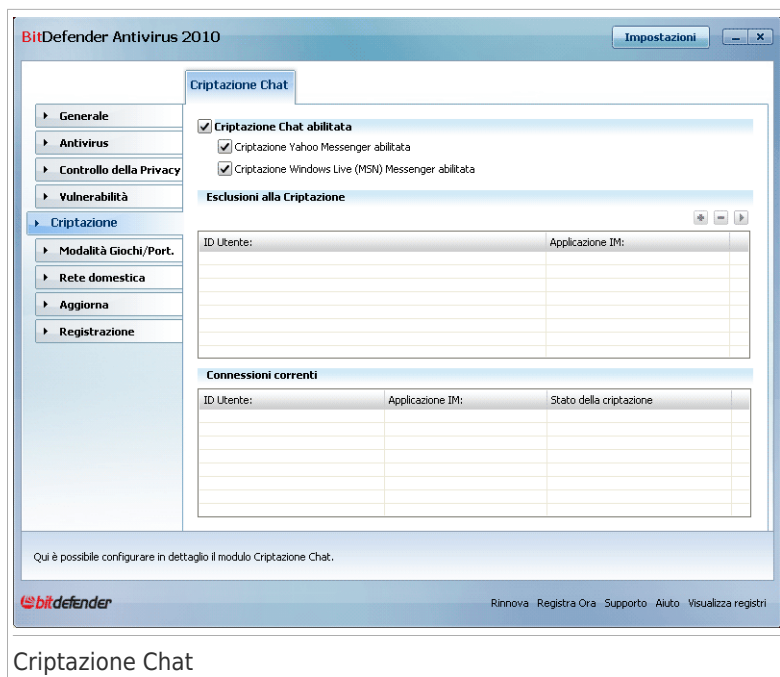
- Il tuo partner di chat abbia una versione di BitDefender installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

Importante

BitDefender non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o se uno dei partner utilizza Yahoo! e l'altro Windows Live (MSN).

Per configurare la criptazione dell'instant messaging, fare clic su **Criptazione>Criptazione IM** in Modalità Avanzata.

Nota

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di BitDefender nella finestra di chat. Per ulteriori informazioni fare riferimento a *«Integrazione in Programmi Instant Messenger»* (p. 206).

Criptazione Chat

Di default, la Criptazione Chat è abilitata sia per Yahoo Messenger che per Windows Live (MSN) Messenger. Potete scegliere di disabilitare la Critazione Chat solo per una specifica applicazione di chat o completamente.

Vengono mostrate due tabelle:

- **Esclusioni della Criptazione** - elenca le ID degli utenti ed i relativi programmi di chat per i quali la criptazione è disabilitata. Per rimuovere un contatto dall'elenco, selezionarlo e quindi fare clic sul pulsante ⊟ **Rimuovi**.
- **Connessioni Correnti** - elenca le connessioni in corso di chat (ID utente e programma associato) e se queste sono criptate o meno. Una connessione può non essere criptata per questi motivi:
  - Avete esplicitamente disabilitato la criptazione per questo contatto.
  - Il vostro contatto non ha installata una versione di BitDefender che supporti la Criptazione chat.

21.1. Disabilitare la Criptazione per Utenti Specifici

Per disabilitare la criptazione per uno specifico utente, seguire questi passaggi:

1. Fare clic sul pulsante **Aggiungi** per aprire la finestra di configurazione.

Aggiungere Contatti

2. Digitare la ID utente del vostro contatto nel campo corrispondente.
3. Selezionare l'applicazione di instant messaging associata al contatto.
4. Selezionare **OK**.

22. Modalità Gioco / Portatile

La Modalità Gioco / Portatile vi permette di configurare le modalità speciali di operatività di BitDefender:

- Modalità Gioco modifica temporaneamente le impostazioni del prodotto in modo di minimizzare il consumo di risorse mentre giocate.
- Modalità Portatile impedisce che le funzioni programmate vengano eseguite quando il portatile funziona con la batteria in modo da risparmiare energia della batteria.

22.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Tutti gli allarmi e pop-up BitDefender sono disabilitati.
- Il livello di protezione in tempo reale di BitDefender è impostato come **Permissivo**.
- Gli aggiornamenti non vengono eseguiti di default.

Nota
Per cambiare queste impostazioni, cliccare su Aggiornamento > Impostazioni e deselezionare la casella **Non aggiornare se la Modalità Gioco è attiva**.

- Le funzioni di scansione programmate sono disabilitate di default.

Di default, BitDefender entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista BitDefender dei giochi conosciuti o quando un'applicazione passa a schermo pieno. Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. E' fortemente consigliato di uscire dalla Modalità Gioco quando avete finito di giocare (potete usare la stessa hotkey di default `Ctrl+Alt+Shift+G`).

Nota
Mentre siete in Modalità Gioco, potete vedere la lettera G sull'icona BitDefender.

Per configurare la Modalità Gioco, andare su **Modalità Gioco / Laptop>Modalità Gioco** in Modalità Avanzata.

Modalità giochi

Nella parte superiore della sezione è possible vedere lo stato della Modalità Gioco. È possibile fare clic su **Attiva Modalità giochi** o **Disattiva Modalità giochi** per cambiare lo stato attuale.

22.1.1. Configurazione Automatica della Modalità Gioco

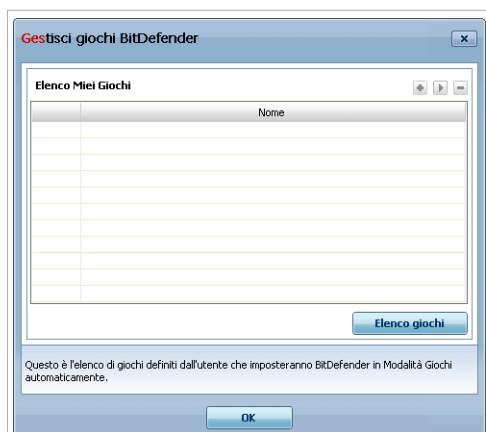
La Modalità Gioco automatica consente a BitDefender di entrare in Modalità Gioco quando un gioco viene rilevato. E' possibile configurare le seguenti opzioni:

- **Usare la lista di default dei giochi fornita da BitDefender** - per entrare automaticamente in Modalità Gioco quando iniziate un gioco della lista dei giochi conosciuti da BitDefender. Per vedere questo elenco, fare clic su **Gestione giochi** e quindi su **Elenco giochi**.
- **Entrare nella Modalità giochi quando una applicazione è a schermo pieno** - per entrare automaticamente nella Modalità giochi quando un'applicazione passa a schermo pieno.
- **Aggiungere l'applicazione alla lista dei giochi?** - perchè vi venga richiesto di aggiungere una nuova applicazione alla lista dei giochi quando abbandonate lo schermo pieno. Aggiungendo una nuova applicazione alla lista dei giochi, la

prossima volta che la avvierete BitDefender entrerà automaticamente in Modalità Gioco.

Nota
Se non desiderate che BitDefender entri automaticamente in Modalità Gioco, deselezionare la casella **Modalità Gioco Automatica**.

22.1.2. Gestione della Lista dei Giochi

BitDefender entra automaticamente in Modalità Gioco quando avviate una applicazione dalla lista dei giochi. Per visualizzare e gestire la lista dei giochi, cliccare su **Gestire Giochi**. Apparirà una nuova finestra.

Lista dei Giochi

Nuove applicazioni vengono automaticamente aggiunte alla lista quando:

- Avviate un gioco dalla lista dei giochi conosciuti di BitDefender. Per visualizzare la lista, fare clic su **Elenco giochi**.
- Dopo aver abbandonato lo schermo pieno, aggiungete l'applicazione alla lista dei giochi dalla finesta proposta.

Se volete disabilitare la Modalità Gioco Automatica per un'applicazione specifica della lista, deselezionare la casella corrispondente. Dovreste disabilitare la Modalità Gioco Automatica per le applicazioni regolari che vanno in schermo pieno, come web browser o movie player.

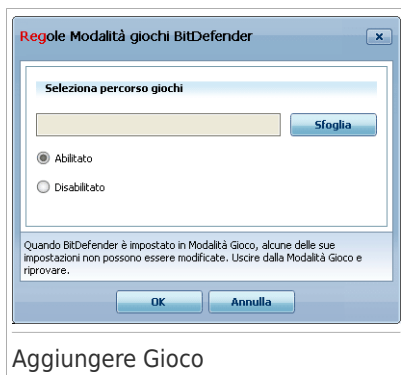
Per gestire questa lista giochi, potete usare i tasti situati nella parte superiore della tabella:

- Cliccare su **OK** per aggiungere la nuova applicazione alla lista dei giochi.

- **Rimuovi** - per rimuovere tutte le applicazioni installate.
- Cliccare su **OK** per aggiungere l'applicazione alla lista dei giochi.

Aggiungere o Modificare Giochi

Quando aggiungete o modificate un'entrata della lista dei giochi, apparirà la seguente finestra:

Aggiungere Gioco

Cliccare su **Sfoglia** per selezionare l'applicazione o digitare il percorso completo dell'applicazione nel campo corrispondente.

Se non si desidera entrare automaticamente in Modalità Gioco quando l'applicazione è già iniziata, selezionare **Disabilitare**.

Cliccare su **OK** per aggiungere l'entrata alla lista dei giochi.

22.1.3. Configurazione delle Impostazioni della Modalità Gioco

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

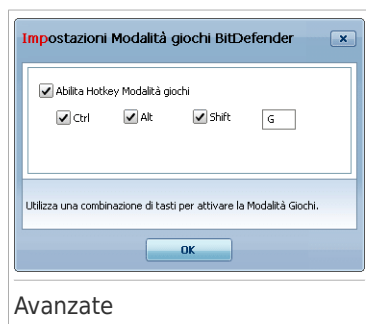
- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità giochi. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Gioco.

22.1.4. Modifica Hotkey della Modalità Gioco.

Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. Per modificare la hotkey, seguire questi passaggi:

1. Cliccare su **Impostazioni Avanzate**. Apparirà una nuova finestra.

Avanzate

2. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:
   - Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
   - Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

   Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

   Nota
   Deselezionare la casella **Usare HotKey** disabiliterà la hotkey.

3. Selezionare **Applica** per salvare le modifiche.

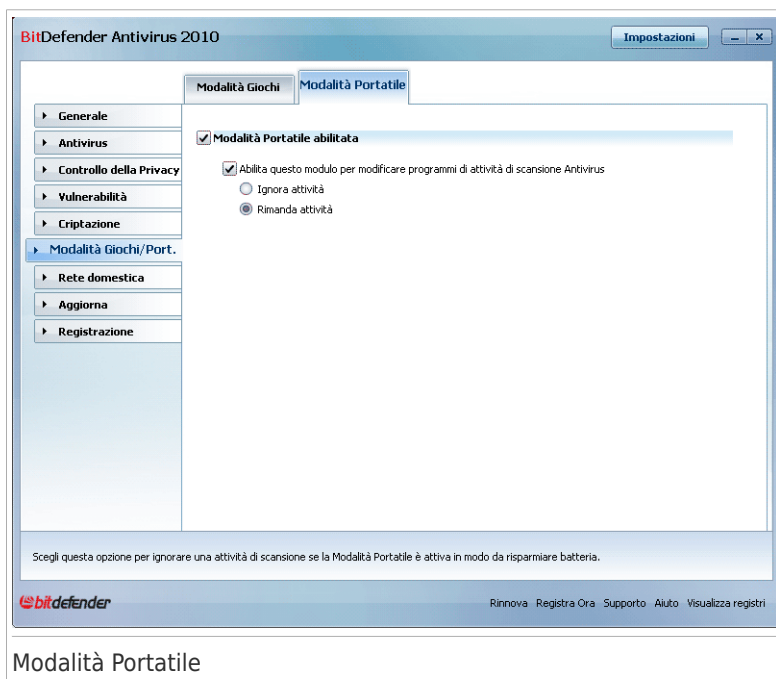
22.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di BitDefender sul consumo di energia mentre questi apparecchi funzionino con la batteria.

Mentre siete in Modalità Portatile, le funzioni programmate non verranno eseguite di default.

BitDefender rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, BitDefender uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per configurare la Modalità Portatile, andare su **Modalità Gioco / Portatile>Modalità Portatile** in Modalità Avanzata.

Modalità Portatile

Potete vedere se la Modalità Portatile è abilitata o meno. Se la Modalità Portatile è abilitata, BitDefender applicherà le impostazioni configurate mentre il portatile lavora con la batteria.

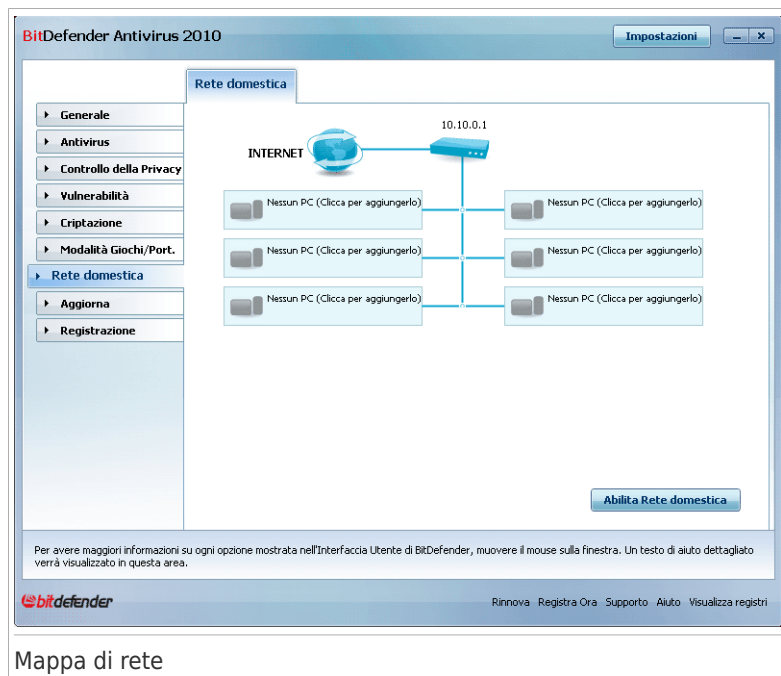
22.2.1. Configurazione delle Impostazioni della Modalità Portatile

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità portatile. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Portatile.

23. Rete domestica

Il modulo Rete vi permette gestire i prodotti BitDefender installati sui computer di casa da un singolo computer.

Mappa di rete

Per essere in grado di gestire i prodotti BitDefender installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica BitDefender sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).
3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

23.1. Unirsi alla Rete BitDefender

Per unirsi alla rete domestica BitDefender, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

23.2. Aggiungere dei computer alla Rete BitDefender

Prima di poter aggiungere un computer alla rete domestica BitDefender dovrete configurare la password per la gestione domestica BitDefender sul rispettivo computer.

Per aggiungere un computer alla rete domestica BitDefender , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.

Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

Indica un computer online senza prodotti BitDefender installati.

Indica un computer online con BitDefender installato.

Indica un computer offline con BitDefender installato.

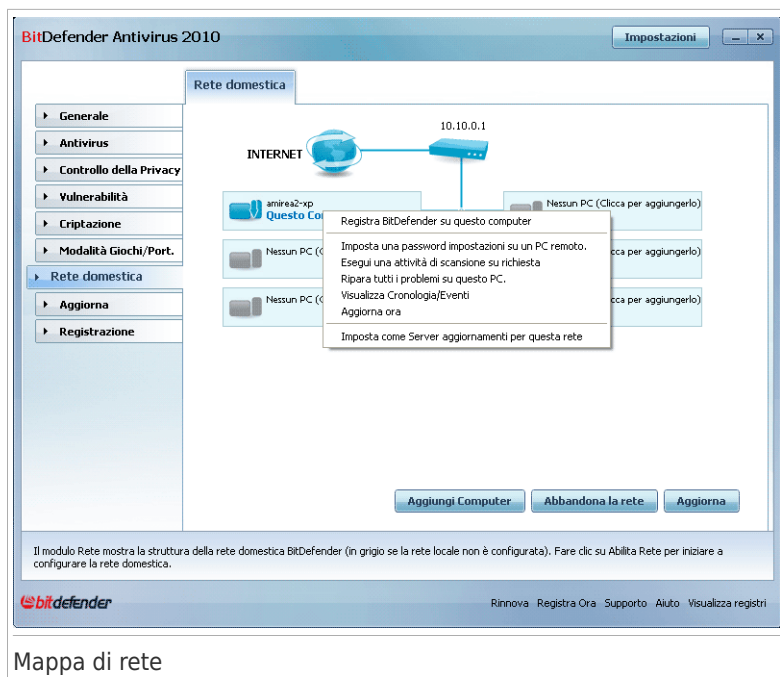
3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.
4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.

Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

23.3. Gestione della Rete BitDefender

Una volta che avete creato con successo una rete domestica BitDefender, potrete gestire tutti i prodotti BitDefender da un singolo computer.

Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema, stato della registrazione di BitDefender).

Se si fa clic sul nome di un computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire sul computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Registra BitDefender su questo computer**

  Permette di registrare BitDefender sul computer inserendo una chiave di licenza.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni BitDefender sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

  Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi Tutti i Problemi.

- **Visualizzare Cronologia/Eventi**

  Permette di accedere al modulo **Cronologia&Eventi** del prodotto BitDefender installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto BitDefender installato sul computer.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti BitDefender installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

Nota

Se programmate di eseguire più funzioni, potete selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

24. Aggiorna

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Se siete connessi ad Internet con banda larga o DSL, BitDefender si prenderà cura di sè da solo. Per default, esso cercherà degli aggiornamenti, ogni volta che avvierete il vostro computer ed ogni **ora**dopo l'avvio.

Se viene rilevato un aggiornamento, vi verrà chiesto di confermare l'aggiornamento o l'aggiornamento verrà eseguito automaticamente, a seconda delle impostazioni dell'aggiornamento automatico update settings.

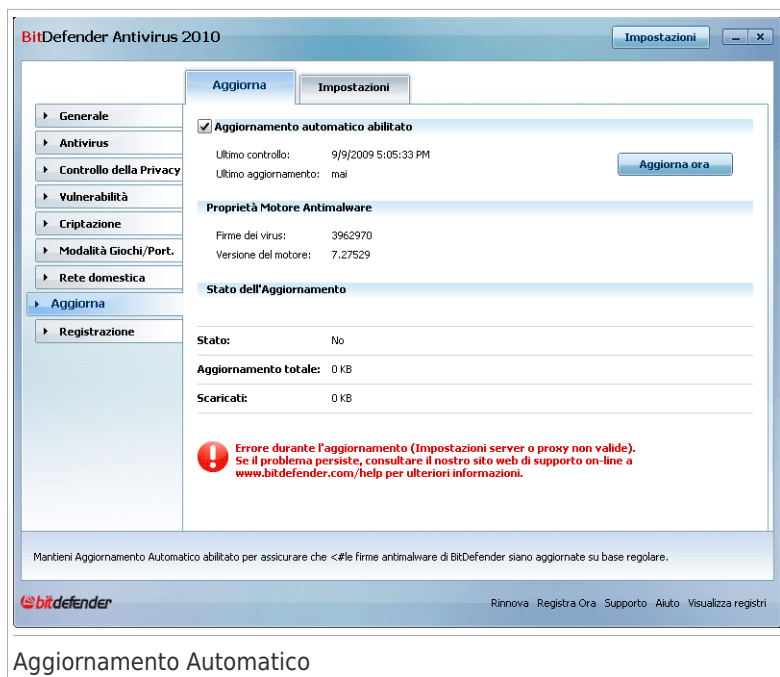
Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Gli Aggiornamenti arrivano nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i file contenenti le impronte dei virus devono essere aggiornati per garantire una protezione aggiornata permanente contro queste nuove minacce. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamento per I motori antispyware** - nuove firme antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Antispyware Update**.
- **Aggiornamenti del Prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorare l'efficienza del prodotto. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

24.1. Aggiornamento Automatico

Per visualizzare informazioni relative all'aggiornamento ed eseguire aggiornamenti automatici, fare clic su **Aggiornamento>Aggiornamento** in Modalità Avanzata.

Aggiornamento Automatico

Qui è possibile visualizzare quando sono stati eseguiti l'ultimo controllo degli aggiornamenti e l'ultimo aggiornamento, così come le informazioni sull'ultimo aggiornamento eseguito (se con successo o gli errori verificatisi). Inoltre si mostrano informazioni sulla versione del motore corrente ed il numero di impronte.

se aprite questa sezione durante un aggiornamento potrete visualizzare lo stato del download.

Importante
Per essere sempre protetti, tenete l' **Aggiornamento Automatico** abilitato.

24.1.1. Richiedere un aggiornamento

L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiornare adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell'utente**.

Il modulo **Aggiornamento** si collegherà al server di aggiornamento di BitDefender e verificherà la disponibilità. Se viene rilevato un aggiornamento, secondo le opzioni impostate nella sezione Impostazioni Aggiornamento Manuale, vi verrà chiesto di confermarlo oppure verrà eseguito automaticamente.

Importante
Può essere necessario riavviare il computer una volta completato l’aggiornamento. Noi consigliamo di farlo al più presto possibile.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l’aggiornamento periodico di BitDefender su richiesta dell’utente.

24.1.2. Disattivare Aggiornamento Automatico

Scegliendo di disattivare l'aggiornamento automatico, apparirà una finestra di avviso. Dovete confermare la vostra scelta selezionando dal menu per quanto tempo volete che l'aggiornamentop automatico venga disattivato. Potete disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
Questa è una questione critica di sicurezza. Vi consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se BitDefender non verrà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

24.2. Impostazioni dell’aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Per default, BitDefender controllerà la disponibilità di aggiornamenti ogni ora sulla Internet ed installerà gli aggiornamenti disponibili senza avvisarvi.

Per configurare le impostazioni di aggiornamento e gestire i proxy, fare clic su **Aggiornamento>Impostazioni** in Modalità Avanzata.

Impostazioni dell'aggiornamento

Le impostazioni dell'aggiornamento sono ragruppate in 4 categorie (**Impostazioni Ubicazione Aggiornamento**, **Impostazioni Aggiornamento Automatico**, **Impostazioni Aggiornamento Manuale** ed **Impostazioni Avanzate**). Ogni categoria verrà descritta separatamente.

24.2.1. Impostare Ubicazioni Aggiornamento

Per configurare le ubicazioni dell'aggiornamento utilizzare le opzioni della categoria **Impostazioni Ubicazione Aggiornamento**.

Nota

Configurare queste impostazioni solo se siete connessi ad una rete locale che immagazzini localmente le impronte malware di BitDefender o se vi connettete ad Internet attraverso un server proxy.

Per aggiornamenti più affidabili e veloci, potete configurare due ubicazioni per l'aggiornamento: **Ubicazione principale dell'aggiornamento** e **Ubicazione alternativa dell'aggiornamento**. Di default, queste ubicazioni sono la stessa:`http://upgrade.bitdefender.com`.

Per modificare una delle ubicazioni dell'aggiornamento, inserire l'URL dello specchio locale nel campo **URL** corrispondente all'ubicazione che si desidera modificare.

Nota

Vi consigliamo di impostare come ubicazione principale dell'aggiornamento lo specchio locale e di non modificare l'ubicazione alternativa, come piano di sicurezza interna nel caso in cui lo specchio locale non fosse disponibile.

Nel caso in cui l'azienda usi un server proxy per connettersi ad internet, selezionare **Usa proxy** e poi fare clic su **Impostazioni proxy** per configurare le impostazioni proxy. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Gestione Proxies»* (p. 193)

24.2.2. Configurazione Aggiornamento Automatico

Per configurare l'esecuzione automatica del processo di aggiornamento da parte di BitDefender, utilizzare le opzioni della categoria **Impostazioni Aggiornamento Automatico**.

È possibile specificare il numero di ore tra due controlli consecutivi per aggiornamenti nel campo **Aggiorna ogni**. Per default l'intervallo di tempo tra aggiornamenti è impostato ad un'ora.

Per specificare come dovrebbe essere eseguito il processo di aggiornamento automatico, selezionare una delle seguenti opzioni:

- **Aggiornamento silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.
- **Chiedere prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.

24.2.3. Configurazione Aggiornamento Manuale

Per specificare come dovrà essere eseguito l'aggiornamento manuale (aggiornamento a richiesta dell'utente) selezionare una delle seguenti opzioni dalla categoria **Impostazioni Aggiornamento Manuali**:

- **Aggiornamento silenzioso** - l'aggiornamento manuale verrà eseguito automaticamente in background, senza l'intervento dell'utente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.

24.2.4. Configurazione delle Impostazioni Avanzate

Per evitare che il processo di aggiornamento di BitDefender interferisca con il vostro lavoro, configurare le opzioni nella categoria **Impostazioni Avanzate**:

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi file finche il sistema venga riavviato. Non verrà chiesto all'utente di riavviare, a fin che il processo di aggiornamento non interferisca con il lavoro dell'utente.
- **Non aggiornare se la scansione è attiva** - BitDefender non verrà aggiornato se è in corso un processo di scansione. In tal modo la procedura di aggiornamento BitDefender non interferisce con le operazioni di scansione.

Nota
Se BitDefender è aggiornato durante una scansione, la procedura di scansione viene interrotta.

- **Non aggiornare se la modalità gioco è attiva** - BitDefender non eseguirà l'aggiornamento se la modalità gioco è attiva. In questo modo si può minimizzare l'influenza del prodotto sulla performance del vostro sistema durante i giochi.

24.2.5. Gestione Proxies

Se la vostra azienda utilizza un server proxy per connettersi ad Internet, dovrete specificare le impostazioni di proxy perchè BitDefender si possa aggiornare da solo. Altrimenti, esso utilizzerà le impostazioni proxy dell'amministratore che installò il prodotto o, se ci sono, le impostazioni predefinite del browser dell'utente corrente.

Nota
Le impostazioni del proxy possono essere configurate solo da utenti con diritti di amministratore sul computer oppure da "power users" (utenti che conoscono la password per le impostazioni del prodotto).

Per gestire le impostazioni proxy, fare clic su **Impostazioni Proxy**. Apparirà una nuova finestra.

Gestore del proxy

Vi sono tre gruppi di impostazioni del proxy:

- **Proxy rilevato al momento dell'installazione)** - impostazioni del proxy rilevate sull'account dell'amministratore durante l'installazione le quali possono essere configurate solo utilizzando tale account. Se il server proxy richiede un nome utente ed una password, specificarli nei rispettivi campi.
- **Proxy del browser predefinito** - impostazioni proxy dell'utente attuale, tratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, è necessario specificarle nei campi corrispondenti.

Nota

I browser web supportati sono Internet Explorer, Mozilla Firefox ed Opera. Se usate un altro browser di default, BitDefender non sarà in grado di ottenere le impostazioni del proxy dell'utente corrente.

- **Proxy personalizzato** - impostazioni del proxy che si possono configurare se si accede come amministratore.

  Le seguenti impostazioni devono essere specificate:
  - **Indirizzo** - inserire l'IP del server proxy.
  - **Porta** - inserire la porta che utilizza BitDefender per connettersi al server proxy.
  - **Nome Utente** - inserire un nome utente riconosciuto dal proxy.
  - **Password** - inserire la password valida per l'utenza, già specificata precedentemente.

Quando ci si tenta di connettere ad Internet, ogni set di impostazione del proxy viene tentato uno alla volta, finchè BitDefender non riesce a connettersi.

In primo luogo verrà usato il set contenente le vostre impostazioni per connettersi ad Internet. Se questo non funzionasse, verranno utilizzate successivamente le impostazioni del proxy rilevate al momento dell'installazione. Ed infine, se neanche queste funzionassero, le impostazioni del proxy dell'utente corrente verranno ricavate dal browser predefinito ed utilizzate per connettersi ad Internet.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Selezionare **Applica** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

25. Registrazione

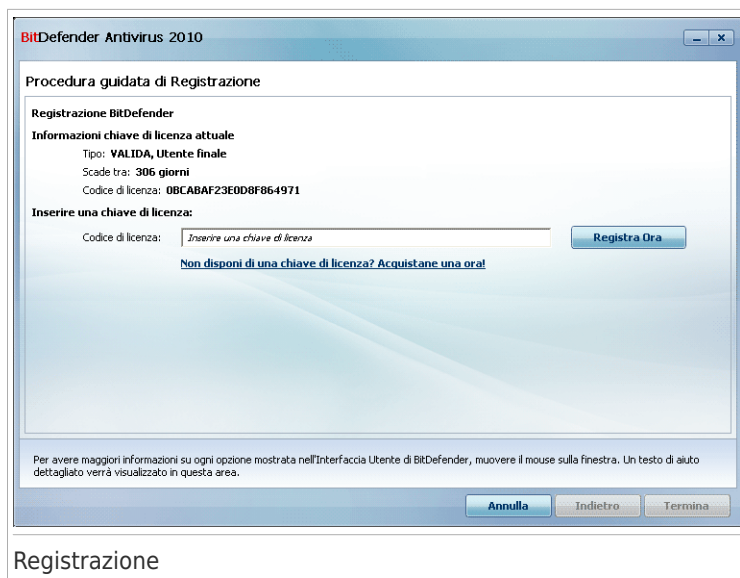
Per trovare informazioni complete sul vostro prodotto BitDefender e sullo stato della registrazione, fare clic su **Registrazione** in Modalità Avanzata.

Registrazione

Questa sezione mostra:

- **Informazioni sul Prodotto**: il prodotto BitDefender e la versione.
- **Informazioni sulla Registrazione**: l'indirizzo mail usato per registrare il vostro account BitDefender (se configurato), la chiave di licenza attuale e quanti giorni mancano fino alla scadenza della licenza.

25.1. Registrazione di BitDefender Antivirus 2010

Fare clic su **Registra Ora** per aprire la finestra di registrazione del prodotto.

Registrazione

Potete vedere lo stato della registrazione BitDefender, la chiave di licenza corrente ed i giorni mancanti alla scadenza della licenza.

Per registrare BitDefender Antivirus 2010:

1. Inserire la chiave di licenza nel campo di modifica.

Nota
Potete trovare la vostra chiave di licenza:
- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

2. Fare clic su **Registra Ora**.
3. Selezionare **Termina**.

25.2. Creazione di un Account BitDefender

Come parte del processo di registrazione, è necessario creare un account BitDefender L'account BitDefender ti da accesso a supporto tecnico gratis ed a offerte speciali e promozioni. Se avete perso la vostra chiave di licenza BitDefender, potete logarvi sul vostro conto in http://myaccount.bitdefender.com per recuperarla.

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Se non si è ancora creato un account BitDefender, fare clic su **Attiva Prodotto** per aprire la finestra di registrazione del prodotto.

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 198)
- «Ho già un account BitDefender» (p. 199)

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.

- **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
- **Confermare Password** - inserire di nuovo la password specificata previamente.

Nota

Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Nota

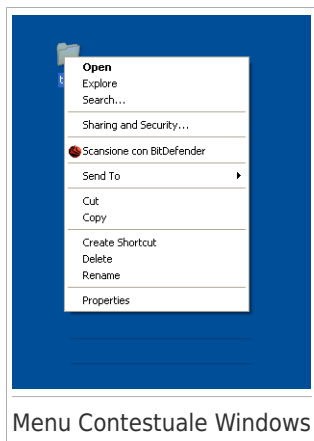
Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

Integrazione in Software Windows e di terzi

26. Integrazione nel Menu Contestuale Windows

Il menu contestuale Windows appare ogni volta che si fa clic con il pulsante destro su un file o una cartella del computer o un oggetto sul desktop.

Menu Contestuale Windows

BitDefender si integra nel menu contestuale Windows per aiutare a scansionare file in cerca di virus. È possibile individuare una opzione BitDefender sul menu contestuale cercando l'icona BitDefender.

26.1. Scansiona con BitDefender

È semplice eseguire la scansione di file, cartelle e persino dischi rigidi interi utilizzando il menu contestuale Windows. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con BitDefender**. Lo Scanner BitDefender apparirà e vi guiderà attraverso il processo di scansione.

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti.

Per modificare le opzioni di scansione, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**.

4. Fare clic con il tasto destro sull'attività **Scansione contestuale** e selezionare **Apri**. Apparirà una finestra.
5. Fare clic su **Personalizza** e configurare le opzioni di scansione come necessario. Per scoprire cosa fa una opzione, posizionare il mouse su di essa e leggere la descrizione visualizzato nel fondo della finestra.
6. Selezionare **Applica** per salvare le modifiche.
7. Fare clic su**OK** per confermare e applicare le nuove opzioni di scansione.

Importante

Non si dovrebbero modificare le opzioni di scansione di questo metodo di scansione a meno che non vi siano ragioni valide per farlo.

27. Integrazione nei Web Browser

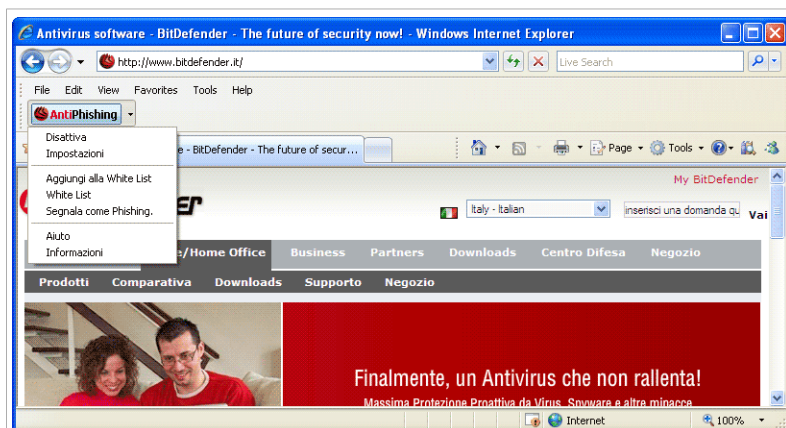
BitDefender vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da BitDefender.

BitDefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox

Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nei web browser citati sopra.

La barra degli strumenti antiphishing, rappresentata dall'icona BitDefender, si trova nella parte superiore del browser. Cliccare sopra per aprire il menu della barra degli strumenti.

Nota
Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti BitDefender**.

Barra degli Strumenti Antiphishing

Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la protezione Antiphishing di BitDefender nel browser web attuale.

- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing. Sono disponibili le seguenti opzioni:
  - **La protezione Web Antiphishing in tempo reale** - individua e avverte in tempo reale se un sito web è oggetto di phishing (impostato per rubare informazioni personali). Questa opzione controlla la protezione antiphishing BitDefender solo nel browser web attuale.
  - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.

Nota

Aggiungere un sito alla White List significa che BitDefender non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **White List** - apre la White List.

White List Antiphishing

Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing BitDefender. Se si vuole rimuovere un sito dalla White List in modo che sia notificata qualsiasi minaccia di phishing su quella pagina, fare clic sul pulsante **Rimuovi** a fianco.

Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.

- **Segnala come phishing** - informa il Laboratorio BitDefender che si considera il relativo sito web come sito usato per phishing. Segnalando siti web di phishing si aiuta a proteggere altri da furti di identità.
- **Aiuto** - apre la documentazione elettronica.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

28. Integrazione in Programmi Instant Messenger

BitDefender offre delle capacità di criptazione per proteggere i vostri documenti confidenziali e le vostre conversazioni attraverso Yahoo Messenger e MSN Messenger.

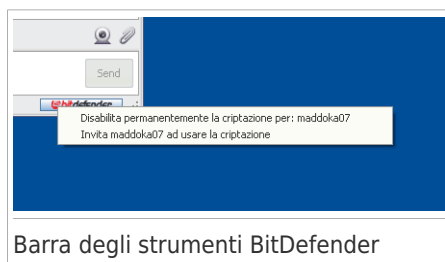
Di default, BitDefender esegue la criptazione di tutte le vostre sessioni chat, purché:

- Il tuo partner di chat abbia una versione di BitDefender installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

Importante

BitDefender non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o altra applicazione chat che supporti Yahoo Messenger o MSN.

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di BitDefender nella finestra di chat. La barra degli strumenti dovrebbe essere posizionata in basso a destra della finestra chat. Cercare il logo BitDefender per trovarla.

Barra degli strumenti BitDefender

Nota

La barra degli strumenti indicate che una conversazione è criptata mostrando una piccola chiave vicino al logotipo BitDefender.

Facendo clic sulla barra degli strumenti di BitDefender appaiono le seguenti opzioni:

- **Disabilita criptazione per sempre per `contatto`.**
- **Invita `contatto` ad usare la criptazione.** Per criptare le conversazioni, il contatto deve installare BitDefender e utilizzare un programma IM compatibile.

Come fare

29. Scansione di file e cartelle

La scansione è facile e flessibile con BitDefender. Ci sono 4 modi per impostare BitDefender a scansionare file e cartelle per virus e altro malware:

- Utilizzando il Menu Contestuale Windows
- Utilizzando attività di scansione
- Utilizzando la scansione manuale BitDefender
- Utilizzando la barra attività di scansione

Una volta avviata la scansione, apparirà la procedura guidata di Scansione che illustra il processo. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 53).

29.1. Utilizzando il Menu Contestuale Windows

Si tratta del modo più semplice e consigliato per scansionare un file o una cartella sul computer. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con BitDefender**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Tipiche situazioni in cui si userebbe questo metodo includono:

- Si sospetta che un file o una cartella specifica sia infetta.
- Ogni volta che si scarica un file di Internet che potrebebro essere pericolosi.
- Scansionare una condivisione di rete prima di copiare i file sul computer.

29.2. Utilizzando attività di scansione

Se si desidera scansionare il computer o cartelle specifiche regolarmente, si consiglia di considerare l'utilizzo delle attività di scansione. Le attività di scansione istruisce BitDefender in merito a quali ubicazioni scansionare, e quali opzioni di scansione e azioni applicare. Inoltre, è possibile programmare tali azioni per eseguirle regolarmente o in momenti specifici.

Per scansionare il computer utilizzando attività di scansione, è necessario aprire l'interfaccia BitDefender ed eseguire le attività di scansione desiderate. A seconda della modalità di visualizzazione dell'interfaccia, si devono eseguire differenti passi per eseguire attività di scansione.

Esecuzione attività di scansione nella modalità inesperto

Nella modalità inesperto, è possibile eseguire solo una scansione di tutto il computer facendo clic su **Scansiona ora**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Esecuzione attività di scansione nella modalità intermedia

Nella Modalità Intermedia, è possibile eseguire diverse attività di scansione pre-configurate. È possibile inoltre configurare ed eseguire scansioni personalizzate per scansionare ubicazioni specifiche sul computer usando opzioni di scansione personalizzate. Eseguire questi passi per eseguire una attività di scansione nella Modalità Intermedia:

1. Fare clic sulla scheda **Antivirus**.
2. Sulla sinistra dell'area Attività veloci, fare clic su **Scansione del sistema** per avviare una scansione standard di tutto il computer. Per eseguire una attività di scansione differente, fare clic sulla freccia sul fondo e selezionare l'attività di scansione desiderata. Per configurare ed eseguire una scansione personalizzata, fare clic su **Scansione Personalizzata**. Queste sono le attività di scansione disponibili:

Funzione di Scansione	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.
Personalizzare Scansione	Questa opzione permette di configurare ed eseguire un'attività di scansione personalizzata, permettendo di specificare cosa esaminare e quali opzioni generali di scansione utilizzare. È possibile salvare le attività di scansione personalizzate in modo da poterle utilizzare di nuovo in Modalità Intermedia o Avanzata.

3. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione. Se si sceglie di eseguire una scansione personalizzata, è necessario completare l'assistente Scansione Personalizzata.

Esecuzione attività di scansione in Modalità Avanzata

In Modalità avanzata è possibile eseguire tutte le attività di scansione pre-configurate e modificare le opzioni di scansione. Inoltre è possibile creare attività di scansione personalizzate se si desidera scansionare parti specifiche del computer. Eseguire questi passi per eseguire un'attività di scansione in Modalità Avanzata:

1. Clicca su **Antivirus** dal menù a sinistra.
2. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione. Queste sono le attività di scansione predefinite che si possono utilizzare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

3. Fare un doppio clic sull'attività di scansione che si desidera eseguire.
4. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

29.3. Utilizzo della Scansione Manuale di BitDefender

La scansione Manuale BitDefender consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a

rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando BitDefender Manual Scan.

Per scansionare il computer utilizzando la Scansione Manuale di BitDefender, eseguire i seguenti passi:

1. Sul menu start Start di Windows, seguire il percorso **Start** → **Tutti i programmi** → **BitDefender 2010** → **Scansione manuale di BitDefender** . Apparirà una nuova finestra.
2. Fare clic su **Aggiungi Cartella** per selezionare l'obbiettivo della scansione. Apparirà una nuova finestra.
3. Selezionare il target di scansione:
   - Per eseguire una scansione del desktop, selezionare **Desktop**.
   - Per scansionare un'intera partizione di un disco rigido, selezionarla da Risorse del computer.
   - Per scansionare una cartella specifica, cercare tale cartella e selezionarla.
4. Selezionare **OK**.
5. Fare clic su **Continua** per avviare la scansione.
6. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usata principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

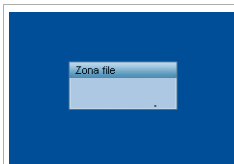
Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

29.4. Utilizzo della Barra delle Attività di Scansione

Barra di Attività della Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Trascinare il file o la cartella che si desidera scansionare sulla barra delle attività di scansione. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Nota

Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 30).

30. Programmazione della scansione del computer

Scansionare il computer periodicamente è il modo migliore per assicurare che il computer non abbia malware. BitDefender consente di programmare attività di scansioni di modo che sia possibile scansionare automaticamente il computer.

Per programmare BitDefender affinché scansioni il computer, eseguire i seguenti passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione.
   - Le attività di sistema sono disponibili e possono essere eseguite da ogni account utente Windows.
   - Le attività dell'utente sono disponibili solo all'utente che le ha create che è l'unico che le può eseguire.

   Queste sono le attività di scansione predefinite che si possono programmare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione Autologon	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Per utilizzare queste attività, è necessario programmarle per farle eseguire all'avvio del sistema. Di default, la scansione autologon è disabilitata
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà

Funzione di Default	Descrizione
	la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

Se nessuna di queste scansioni soddisfa le proprie esigenze, è possibile creare una nuova attività di scansione, che è poi possibile programmare per l'esecuzione come necessario.

4. Fare clic sulla attività do scansione desiderata e selezionare **Programma**. Apparirà una nuova finestra.
5. Programmare l'attività per l'esecuzione come necessario:
   - Per eseguire l'attività di scansione solo una volta, selezionare **Una volta** e specificare la data e l'ora di avvio.
   - Per eseguire l'attività di scansione dopo l'avvio del sistema, selezionare **All'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.
   - Per eseguire l'attività di scansione regolarmente, selezionare **Periodicamente** e specificare la frequenza, la data e l'ora di avvio.

Nota

Ad esempio, per scansionare il computer ogni sabato alle 2 di notte, è necessario configurare la programmazione nel seguente modo:

a. Selezionare **Periodicamente**.

b. Nel campo **Ogni**, digitare 1 e poi selezionare **settimane** dal menu. In questo modo l'attività viene eseguita una volta alla settimana.

c. Impostare come data di inizio il prossimo sabato.

d. Impostare come ora di inizio `2:00:00`.

6. Fare clic su **OK** per salvare la programmazione. L'attività di scansione verrà eseguita automaticamente in base alla programmazione definita. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

Risoluzione dei problemi e aiuto

31. Risoluzione dei problemi

In questo capitolo vengono spiegati alcuni problemi che si possono incontrare utilizzando BitDefender e vengono inoltre fornite possibili soluzioni per questi problemi. La maggior parte di questi problemi possono essere risolti tramite una configurazione appropriata delle impostazioni del prodotto.

Se non è possibile trovare il problema qui, o se la soluzione fornita non lo risolve, è possibile contattare un rappresentante del supporto tecnico di BitDefender come delineato nel capitolo «*Supporto*» (p. 221).

31.1. Problemi di installazione

Quest'articolo permette di risolvere i problemi di installazione più comuni di BitDefender. Tali problemi possono essere raggruppati nelle seguenti categorie:

- Errori di convalida dell'installazione: non è possibile eseguire l'assistente di setup a causa di condizioni specifiche del sistema.
- Installazione non riuscita: l'installazione è stata avviata dall'assistente di setup ma non è stata completata con successo.

31.1.1. Errori di convalida dell'installazione

Quando viene avviato l'assistente di setup vengono verificate diverse condizioni al fine di convalidare la possibilità di avviare l'installazione. La tabella seguente presenta gli errori di convalida dell'installazione più comuni e le soluzioni per superarli.

Errore	Descrizione e soluzione
Non si dispone di privilegi sufficienti per installare il programma.	Per eseguire l'assistente di setup e installare BitDefender è necessario avere privilegi di amministratore. Eseguire una delle seguenti azioni: ● Accedere ad un account di amministratore di Windows ed eseguire di nuovo l'assistente di setup. ● Fare clic con il pulsante destro sul file di installazione e selezionare **Esegui come**. Digitare il nome utente e la password di un account di amministratore di Windows sul sistema.
Il programma di installazione ha individuato una versione precedente di BitDefender che non è stata disinstallata correttamente.	BitDefender era precedentemente installato sul sistema, ma l'installazione non è stata rimossa completamente. Questa condizione blocca la nuova installazione di BitDefender.

Errore	Descrizione e soluzione
	Per risolvere questo errore ed installare BitDefender, seguire questi passi: 1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer. 2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. 3. Riavviare il computer. 4. Avviare di nuovo l'assistente setup per installare BitDefender.
Il prodotto BitDefender non è compatibile con il sistema operativo.	Si sta cercando di installare BitDefender su un sistema operativo non supportato. Controllare i *«Requisiti del sistema»* (p. 2) per scoprire su quali sistemi operativi è possibile installare BitDefender. Se il sistema operativo è Windows XP con Service Pack 1 o senza alcun service pack, è possibile installare il Service Pack 2 o superiore e quindi eseguire di nuovo l'assistente di setup.
Il file di installazione è progettato per un tipo diverso di processore.	Se viene ricevuto tale errore, significa che si sta tentando di eseguire una versione non corretta del file di installazione. Esistono due versioni del file di installazione di BitDefender: una per processori a 32 bit e l'altra per processori a 64 bit. Per assicurarsi di avere la versione corretta per il proprio sistema, scaricare il file di installazione direttamente da www.bitdefender.it.

31.1.2. Installazione non riuscita

Vi sono diverse possibilità di installazione non riuscita:

- Durante l'installazione appare una schermata di errore. Potrebbe essere richiesto di annullare l'installazione oppure potrebbe esservi un pulsante per avviare lo strumento di disinstallazione in modo da pulire il sistema.

Nota
Immediatamente dopo aver avviato l'installazione si potrebbe ricevere una notifica di spazio libero insufficiente su disco per l'installazione di BitDefender. In tal caso liberare lo spazio richiesto sulla partizione dove si desidera installare BitDefender e quindi riprendere o riavviare l'installazione.

- L'installazione si blocca e il sistema potrebbe congelarsi. Solo un riavvio ripristina la capacità di rispondere del sistema.
- L'installazione è stata completata ma è impossibile utilizzare alcune o tutte le funzioni di BitDefender.

Per risolvere un'installazione non riuscita ed installare BitDefender, seguire questi passi:

1. **Ripulire il sistema dopo l'installazione non riuscita.** Se l'installazione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per questa ragione è necessario rimuoverle prima di tentare nuovamente di installare il prodotto.

   Se la schermata di errore fornisce un pulsante per avviare lo strumento di disinstallazione, fare clic su tale pulsante per ripulire il sistema. Altrimenti procedere nel modo seguente:

   a. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.

   b. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore.

   c. Riavviare il computer.

2. **Controllare le possibili cause per il fallimento dell'installazione.** Prima di procedere con la disinstallazione del prodotto, controllare e rimuovere le possibili condizioni che potrebbero aver causato il fallimento dell'installazione:

   a. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.

   b. È anche necessario controllare che il sistema non sia infetto. Eseguire una delle seguenti azioni:

      - Utilizzare il CD di Ripristino di BitDefender per esaminare il computer e rimuovere qualsiasi minaccia esistente. Per ulteriori informazioni fare riferimento a «CD di soccorso BitDefender» (p. 224).
      - Aprire Internet Explorer, andare su www.bitdefender.it ed eseguire una scansione on-line (fare clic sul pulsante **scansione on-line**).

3. Riprovare ad installare BitDefender. Si raccomanda di scaricare ed eseguire la versione più recente del file di installazione da www.bitdefender.it.

4. Se l'installazione non riesce di nuovo, contattare BitDefender per avere assistenza come descritto in «*Supporto*» (p. 221).

31.2. I servizi BitDefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui *I servizi BitDefender non funzionano*. Si potrebbe trovare questo errore:

- L'icona BitDefender nell'area di notifica è grigia e un pop-up informa che i servizi BitDefender non rispondono.
- La finestra BitDefender mostra che i servizi BitDefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- Si sta installando un aggiornamento importante.
- errori temporanei di comunicazione tra i servizi di BitDefender.
- alcuni servizi di BitDefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul computer contemporaneamente a BitDefender.
- virus presenti nel sistema stanno interferendo con il normale funzionamento di BitDefender.

Per risolvere questo errore, provare queste soluzione:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il computer e aspettare alcuni attimi fino a quando BitDefender è caricato. Aprire BitDefender per vedere se l'errore persiste. Riavviare il computer di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.
4. Se l'errore persiste, potrebbe essere un problema più serio (ad esempio, ci potrebbe essere un virus che interferisce con BitDefender). Rivolgersi a BitDefender per supporto come descritto nella sezione «*Supporto*» (p. 221).

31.3. Rimozione di BitDefender non riuscita

Questo articolo permette di risolvere gli errori che potrebbero verificarsi nella rimozione di BitDefender. Vi sono due possibili situazioni:

- Durante la rimozione appare una schermata di errore. La schermata fornisce un pulsante per avviare uno strumento di disinstallazione che pulirà il sistema.
- La rimozione si blocca e il sistema potrebbe congelarsi. Fare clic su **Annulla** per annullare la rimozione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per rimuovere completamente BitDefender dal sistema è necessario avviare lo strumento di disinstallazione.

Se la rimozione non riesce con una schermata di errore, fare clic sul pulsante per avviare lo strumento di disinstallazione e ripulire il sistema. Altrimenti procedere nel modo seguente:

1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.
2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.
3. Riavviare il computer.

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione «*Supporto*» (p. 221).

32. Supporto

In veste di stimato fornitore, BitDefender si sforza di fornire ai propri clienti un livello senza pari di supporto veloce e accurato. Il centro di conoscenza BitDefender fornisce articoli che contengono soluzioni alla maggior parte dei problemi e delle domande relative a BitDefender. Se non si riesce a trovare una soluzione nel centro di conoscenza BitDefender, è possibile contattare il Servizio clienti BitDefender. Il nostro rappresentate del supporto risponderà alle domande in tempo e vi fornirà tutta l'assistenza necessaria.

32.1. BitDefender Knowledge Base(Archivio D'informazione BitDefender)

L' Archivio D'informazione BitDefender è un deposito d'informazione sui prodotti BitDefender. Conserva, in un formatto facilmente accessibile, rapporti sui risultati del supporto tecnico in corso ed attività di disinfezione dei team di supporto e sviluppo di BitDefender , assieme a più articoli su prevenzione virus, la gestione delle soluzioni BitDefender e spiegazioni dettagliate, e tanti altri articoli.

L'Archivio D'informazione BitDefender è aperto al pubblico e gratuitamente esplorabile. Questa ricchezza d'informazione è un altro modo ancora di fornire ai clienti di BitDefender dalle conoscenze tecniche e comprensione necessarie. Tutte le richieste valide d'informazione o rapporti su difetti, provenienti di clienti di BitDefender trovano prima o poi la loro strada fino al'Archivio D'informazione BitDefender, come rapporti di disinfezione, dei modi di aggirare le truffe, o articoli informativi, in modo di supplementare i file di aiuto dei prodotti.

L' Archivio D'informazione BitDefender è disponibile in qualsiasi momento su http://kb.bitdefender.com.

32.2. Chiedere Aiuto

Per richiedere aiuto, si deve utilizzare il Self-Service Web BitDefender. Eseguire i seguenti passi:

1. Visitare http://www.bitdefender.com/help. Qui è possibile trovare il Centro di conoscenza BitDefender. Il Centro di conoscenza BitDefender include numerosi articoli che contengono soluzioni per questioni relative a BitDefender.
2. Fare una ricerca del Centro di conoscenza BitDefender per articoli che potrebbero fornire una soluzione al problema.
3. Leggere l'articolo pertinente e provare la soluzione proposta.
4. Se questa soluzione non risolve i tuoi problemi, utilizzare il link nell'articolo per contattare il Servizio clienti BitDefender.
5. Accedere all'account di BitDefender.

6. Contatta un rappresentante di supporto BitDefender tramite e-mail, chat o telefono.

32.3. Informazioni di Contatto:

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partners, sforzandosi costantemente per una comunicazione sempre più efficiente. Se avete delle domande o richieste, non esitare a contattarci.

32.3.1. Indirizzi Web

Dipartimento vendite: sales@bitdefender.com
Supporto tecnico: www.bitdefender.com/help
Documentazione: documentation@bitdefender.com
Programma partner: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Rapporti con i Media: pr@bitdefender.com
Opportunità di lavoro: jobs@bitdefender.com
Invio virus: virus_submission@bitdefender.com
Invio spam: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Pagina web del prodotto: http://www.bitdefender.it
Archivi ftp del prodotto: ftp://ftp.bitdefender.com/pub
Distributori locali: http://www.bitdefender.it/site/Partnership/list/
Archivio D'informazione BitDefender: http://kb.bitdefender.com

32.3.2. Uffici BitDefender

Gli uffici (succursali) di BitDefender sono pronti a rispondere a qualunque richiesta riguardo le loro aree di operazioni, in materie commerciale e generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefono (ufficio&vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Supporto tecnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Germany

BitDefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Ufficio: +49 2301 91 84 222
Vendite: vertrieb@bitdefender.de
Supporto tecnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

UK ed Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Mail: info@bitdefender.co.uk
Telefono: +44 (0) 8451-305096
Vendite: sales@bitdefender.co.uk
Supporto tecnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefono: +34 902190765
Vendite: comercial@bitdefender.es
Supporto tecnico: www.bitdefender.es/ayuda
Sito web: http://www.bitdefender.es

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefono vendite: +40 21 2063470
Indirizzo e-mail ufficio vendite: sales@bitdefender.ro
Supporto tecnico: http://www.bitdefender.ro/suport
Sito web: http://www.bitdefender.ro

CD di soccorso BitDefender

33. Panoramica

Antivirus BitDefender 2010 arriva con un CD di avvio (BitDefender Rescue CD), in grado di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti prima che il sistema operativo si avvii.

Dovresti usare il CD di soccorso BitDefender ogni volta che il tuo sistema operativo non lavora correttamente per via di infezioni di virus. Quello succede normalmente quando non usi un prodotto antivirus.

L'aggiornamento delle impronte dei virus è fatta automaticamente, senza l'intervento dell'utente, ogni volta che inizi il CD di soccorso BitDefender.

BitDefender Rescue CD è una distribuzione di Knoppix ri-masterizzato di BitDefender, che integra l'ultima soluzione di sicurezza di BitDefender per Linux nel CD GNU/Linux Knoppix Live, offrendo un antivirus di desktop capace di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti (includendo partizioni NTFS di Windows). Nello stesso tempo BitDefender Rescue CD può essere utilizzato per ripristinare i vostri dati preziosi quando non si può avviare Windows

Nota
Il BitDefender Rescue CD può essere scaricato da: http://download.bitdefender.com/rescue_cd/

33.1. Requisiti del sistema

Prima di avviare BitDefender Rescue CD, dovete innanzitutto verificare se il vostro sistema ha i seguenti requisiti.

Tipo di processore
Compatibile x86, minimo 166 MHz, ma non sperare un alto rendimento in questo caso. Un processore di generazione i686, a 800 MHz sarebbe una scelta migliore.

Memoria
Minimo 512 MB di Memoria RAM (raccomandati 1 GB)

CD-ROM
BitDefender Rescue CD si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS in grado di avviarlo.

Connessione Internet
Anche se BitDefender Rescue CD funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso alcuni server proxy. Di conseguenza, per una protezione aggiornata, la connessione ad Internet è obbligatoria.

Risoluzione grafica
Scheda grafica standard SVGA-compatibile.

33.2. Software Incluso

Il CD di soccorso BitDefender include i seguenti pacchetti software.

Xedit
Questo è un editore di file di testo.

Vim
Questo è un potente editore di file di testo, contenente evidenziatore di sintassi, un GUI, e molto altro.Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Vim.

Xcalc
Questa è una calcolatrice.

RoxFiler
RoxFiler è un veloce e potente gestore di file grafici.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) è un gestore di file text-mode.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MC .

Pstree
Pstree mostra i processi in corso.

Top
Top mostra le funzioni Linux.

Xkill
Xkill blocca tutte le X risorse di un client.

Partition Image
Partition Image vi aiuta a salvare le partizioni nei formati dei file di sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 in un file di immagine. Questo programma può essere utile a fini di backup.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Partimage.

GtkRecover
GtkRecover è una versione GTK del console del programma di recupero. Aiuta a recuperare dei file.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di GtkRecover.

ChkRootKit
ChkRootKit è uno strumento che vi aiuta ad effettuare la scansione del vostro computer in cerca di rootkits.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di ChkRootKit.

Nessus Network Scanner

Nessus è uno scanner di sicurezza remota per Linux, Solaris, FreeBSD, e Mac OS X.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Nessus.

Iptraf

Iptraf è un Software di monitoraggio di rete IP.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iptraf.

Iftop

Iftop mostra l'uso di larghezza di banda su di un interfaccia.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iftop.

MTR

MTR è uno strumento di diagnosi di rete.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MTR .

PPPStatus

PPPStatus mostra le statistiche sul traffico TCP/IP in entrata ed in uscita.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di PPPStatus.

Wavemon

Wavemon è un'applicazione di monitoraggio per dispositivi di rete wireless.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Wavemon.

USBView

USBView mostra informazioni sui dispositivi connessi al bus USB.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di USBView.

Pppconfig

Pppconfig aiuta a configurare automaticamente una connessione dial up ppp.

DSL/PPPoe

DSL/PPPoe configura una connessione PPPoE (ADSL).

I810rotate

I810rotate cambia l'output su video a i810 hardware usando i810switch(1).

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di I810rotate .

Mutt

Mutt è un potente mail client MIME basato su testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mutt.

Mozilla Firefox

Mozilla Firefox è un noto browser web.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mozilla Firefox.

Elinks

Elinks browser di web in modo testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Elinks.

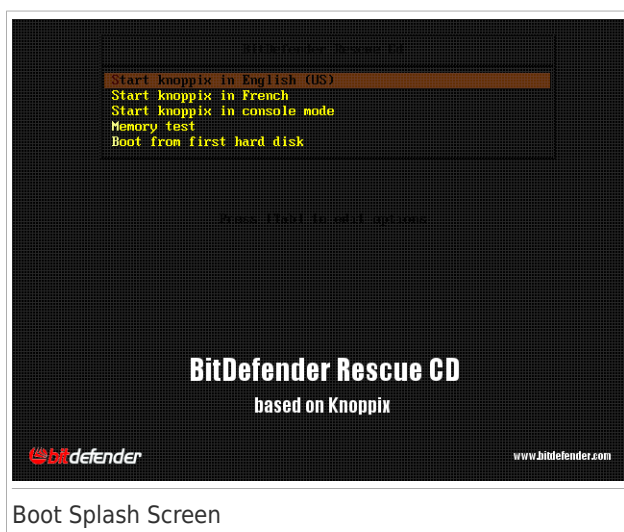
34. BitDefender Rescue CD fai-da-te.

Questo capitolo contiene informazioni su come iniziare e fermare il BitDefender Rescue CD, come eseguire la scansione del vostro computer alla ricerca di malware e anche come salvare dati dal vostro PC Windows compromesso su un dispositivo rimuovibile. In ogni caso, utilizzando le applicazioni software contenute nel CD, potrete eseguire molti processi, la cui descrizione va oltre gli obiettivi di questo manuale.

34.1. Avviare BitDefender Rescue CD

Per avviare il CD, configura il BIOS del tuo computer per avviarsi dal CD, inserisci il CD nell'unità e riavvia il computer. Assicurati che il tuo computer possa avviarsi dal CD.

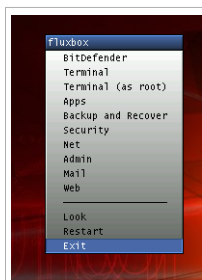
Attendere che venga mostrata la finestra successiva e seguire le istruzioni per avviare BitDefender Rescue CD.

Boot Splash Screen

Al avvio, l'aggiornamento delle impronte dei virus viene eseguito automaticamente. Questo potrebbe richiedere qualche istante.

Quando il processo di avvio è finito si vedrà poi il desktop. Adesso è possibile cominciare ad utilizzare il BitDefender Rescue CD.

Il Desktop

34.2. Arrestare BitDefender Rescue CD

È possibile spegnere il computer in modo sicuro selezionando **Uscire** dal menu contestuale di BitDefender Rescue CD (fare clic con il pulsante destro per aprirlo) o usando il comando **Ferma** su un terminale.

Scegli “Uscire”

Quando BitDefender Rescue CD avrà chiuso tutti i programmi con successo, mostrerà una schermata come l’immagine seguente. Potrete rimuovere il CD per fare l'avvio dall' hard disk. Adesso potete spegnere oppure riavviare il vostro computer.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.......................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.......................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Attendi questo messaggio alla chiusura

34.3. Come eseguo una scansione antivirus?

Apparirà una procedura guidata quando il processo di avvio sarà terminato che permetterà di eseguire una scansione completa del computer. È sufficiente fare clic sul pulsante **Avvia**.

Nota
Se la risoluzione del vostro schermo non è abbastanza alta, vi verrà chiesto di cominciare la scansione in modalità di testo.

Seguire la procedura di tre passi per completare il processo di scansione.

1. Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

   Nota
   La durata del processo dipende dalla complessità della scansione.

2. Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

   I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

   Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.
3. E’ possibile visualizzare il sommario dei risultati.

Se si desidera scansionare solo una certa directory, è possibile utilizzare una delle seguenti alternative:

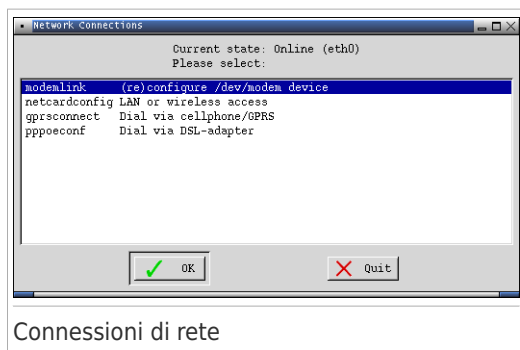
- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul Desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Scanner**, apparirà una nuova finestra.
  3. Selezionare la directory che si desidera scansionare e fare clic su **Apri** per avviare la scansione utilizzando la stessa procedura guidata quando si avviato il computer la prima volta.
- Usare il menu contestuale - cercare le cartelle, fare clic con il pulsante destro su un file o una directory e selezionare **Invia a**. Quindi scegliere **Scanner BitDefender**.
- O puoi emettere questo commando come ruta, da un terminale. Lo **BitDefender Antivirus Scanner** comminciderà con il file o cartella selezionato come ubicazione predefinita da eseguire la scansione.

```
# bdscan /path/to/scan/
```

34.4. Come Configurare la connessione Internet?

Se sei in una rete DHCP ed hai una scheda di rete ethernet, la connessione Internet dovrebbe già essere rilevata e configurata. Per una configurazione manuale, segue questi passi.

1. Cliccare due volte sull'icona Risorse di Rete sul Desktop. Apparirà la seguente finestra.

Connessioni di rete

2. Selezionare il tipo di connessione che state usando e cliccare su OK.

Connessione	Descrizione
modemlink	Selezionare questo tipo di connessione se state usando un modem ed una linea telefonica per accedere ad Internet.
netcardconfig	Selezionare questo tipo di connessione se state usando connessione alla rete locale (LAN) per accedere ad Internet. E' anche adeguato per le connessioni wireless.
gprsconnect	Selezionare questo tipo di connessione se accedete ad Internet tramite rete cellulare usando il protocollo GPRS (General Packet Radio Service). Ovviamente potete anche usare un modem GPRS al posto del cellulare.
pppoeconf	Selezionare questo tipo di connessione se usate un modem DSL (Digital Subscriber Line) per accedere ad Internet.

3. Seguire le istruzioni sullo schermo. Se non siete sicuri di cosa scrivere, contattate il vostro amministratore di sistema o della rete per i dettagli.

Importante

Tenere presente che selezionando una delle opzioni citate sopra attivate solo il modem. Per configurare la connessione di rete, seguire questi passi.

1. Fare clic con il pulsante destro sul desktop. Apparirà il menu contestuale del BitDefender Rescue CD.
2. Selezionare **Terminale (come radice)**.
3. Digitare i seguenti comandi:

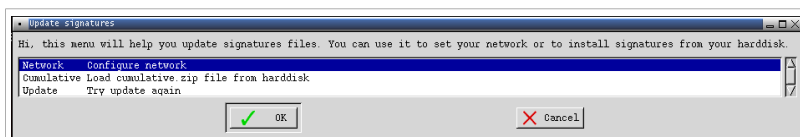
```
# pppconfig
```

4. Seguire le istruzioni sullo schermo. Se non siete sicuri di cosa scrivere, contattate il vostro amministratore di sistema o della rete per i dettagli.

34.5. Come aggiornare BitDefender?

Al momento dell'avvio, l'aggiornamento delle firme virus viene fatto automaticamente. Tuttavia, se si salta questo passo o si desidera semplicemente eseguire un aggiornamento dopo l'avvio, ecco due modi aggiornare BitDefender.

- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Aggiorna**.
- Utilizzare il collegamento **Aggiorna firme** sul desktop.

1. Cliccare due volte sul collegamento sul Desktop Aggiornare Impronte. Apparirà la seguente finestra.

Aggiornare impronte.

2. Eseguire una delle seguenti azioni:
   - Selezionare **Cumulativo** per installare le impronte già salvate sul vostro disco rigido sfogliando il computer e caricando il file `cumulativo.zip`.
   - Selezionare **Aggiornare** per connettersi immediatamente ad Internet e scaricare le impronte di virus più recenti.
3. Selezionare **OK**.

34.5.1. Come aggiornare BitDefender attraverso un proxy?

Se ci fosse un server proxy tra il computer ed Internet, è necessario impostare alcune configurazioni per poter aggiornare le firme dei virus.

Per aggiornare BitDefender su un proxy, utilizzare una delle seguenti opzioni:

- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul Desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Impostazioni**, apparirà una nuova finestra.
  3. In **Aggiorna impostazioni**, selezionare la casella di controllo **Abilita Proxy HTTP**. Specificare l'host Proxy (nel seguente formato: `host[:port]`), l'utente proxy (nel seguente formato: `[domain\]username`) e la password. Selezionare la casella di controllo **Scavalca server proxy quando non è disponibile** per una connessione diretta da utilizzare quando il server proxy non è disponibile.
  4. Fare clic su **Salva**
  5. Fare clic su **Aggiorna**

- Usa terminale (come radice).
  1. Fare clic con il pulsante destro sul desktop. Apparirà il menu contestuale del BitDefender Rescue CD.
  2. Selezionare **Terminale (come radice)**.
  3. Digitare il comando: **cd /ramdisk/BitDefender-scanner/etc**.
  4. Digitare il comando: **mcedit bdscan.conf** per modificare questo file usando GNU Midnight Commander (mc).

5. Cancellare la seguente linea: `#HttpProxy =` (eliminare solo il segno #) e specificare il dominio, nome utente, password e porta del serve proxy. Ad esempio, la linea corrispondente dovrebbe essere così:

   `HttpProxy = myuser:mypassword@proxy.company.com:8080`
6. Premere **F2** per salvare il file corrente, confermare il salvataggio e quindi premere **F10** per chiuderlo.
7. Digitare il comando: **bdscan update**.

34.6. Come posso salvare ai miei dati?

Supponiamo che non potete avviare il vostro PC Windows a causa di problemi sconosciuti. Nello stesso tempo, avete un bisogno disperato di accedere ad alcuni dati importanti sul vostro computer. Questo è il momento in cui BitDefender Rescue CD diventa utile.

Per salvare i vostri dati dal computer ad un dispositivo rimuovibile, come una penna USB, basta seguire questi passaggi:

1. Inserire BitDefender Rescue CD nel lettore CD, la penna USB nella porta USB e quindi riavviare il computer.

Nota

Se inserite la penna USB in un secondo momento, dovrete montare il disco rimovibile seguendo questi passaggi:

a. Cliccare due volte sul collegamento sul Desktop Terminal Emulator.

b. Digitare il seguente comando:

```
# mount  /media/sdb1
```

Tenere presente che a seconda della configuarzione del vostro computer esso potrà essere `sda1` invece di `sdb1`.

2. Attendere finchè BitDefender Rescue CD completi l'avvio. Apparirà la seguente finestra.

Schermo del Desktop

3. Cliccare due volte sulla partizione dove sono ubicati i dati che volete salvare (e.g. `[sda3]`).

Nota

Quando lavorate con BitDefender Rescue CD, avrete a che fare con nomi di partizioni Linux. Quindi, `[sda1]` probabilmente corrisponderà alla partizione Windows `(C:)`, `[sda3]` alla `(F:)`, e `[sdb1]` alla penna USB.

Importante

Se il computer non è stato spento correttamente è possibile che alcune partizioni non siano state montate automaticamente. Per montare una partizione, seguire questi passi.

a. Cliccare due volte sul collegamento sul Desktop Terminal Emulator.
b. Digitare il seguente comando:

```
# mount  /media/partition_name
```

4. Sfogliare le vostre cartelle ed aprire la directory desiderata. Per esempio, `MyData`, contenente le sottodirectory`Movies`, `Music` ed `E-books`.
5. Fare clic con il pulsante destro sulla directory desiderata e selezionare **Copia**. Apparirà la seguente finestra.

Salvataggio dei dati

6. Scrivere `/media/sdb1/` nella corrispondente casella di testo e cliccare **Copiare**.

   Tenere presente che a seconda della configuarzione del vostro computer esso potrà essere `sda1` invece di `sdb1`.

34.7. Come si usa la modalità console?

Se la risoluzione dello schermo non è abbastanza alta per avviare l'interfaccia utente grafica, è possibile eseguire il CD di recupero BitDefender nella modalità console. La modalità testo semplice consente di eseguire una scansione completa del proprio.

Per eseguire il CD nella modalità console, impostare il BIOS del computer per avviarsi dal CD, mettere il CD nel drive e riavviare il computer. Attendere lo schermo di caricamento e selezionare **Avvia knoppix nella modalità console**.

Dopo l'avvio, seguire le istruzioni sullo schermo per eseguire una scansione completa del computer.

BitDefender rileva le partizioni sul proprio disco rigido e aggiorna automaticamente il database delle firme malware prima dell'inizio della scansione. Se vengono trovati dei file infetti, BitDefender li disinfetterà. Dopo il completamento del processo di scansione, viene visualizzato il registro di scansione.

Nota

La durata del processo dipende dalla complessità della scansione.

Glossario

ActiveX

ActiveX è una modalità di scrittura dei Programmi affinché possano essere invocati da altri Programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare dei pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX vengono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

L' adware è spesso combinato con un' applicazione Host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito della applicazione. Non viene commesa quindi alcuna offesa o scortesia.

Comunque, i pop-up di avvertimento possono rappresentare un fastidio, ed in alcuni casi degrada il funzionamento del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo alla privacy degli utenti non completamente ben informati sui termini del'accordo di licenza.

Archivia

Disco, nastro o cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Backdoor

Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del venditore a scopo di manutenzione.

Settore di boot

Settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Virus di boot

Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in

poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni e animazione, nonostante richiedano i plug-in per alcuni formati.

Linea di commando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di commando.

Cookies

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere il proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

I drive di disco possono essere interni (incorporati all'interno di un computer) oppure esterni (collocati in un meccanismo separato e connesso al computer).

Download

Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail
Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.

Eventi
Azione oppure avvenimento rilevato da un programma. Gli eventi possono rappresentare azioni dell'utente, come fare un clic con il mouse o premere un tasto sulla tastiera oppure avvenimenti del sistema, ad esempio memoria insufficiente.

Falso positivo
Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

Estensione del nome di un file
Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da uno a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScipt, "txt" per testi arbitrari.

Euristico
Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

IP
Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Applet Java
Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell'applet e la dimensione (lunghezza e larghezza -in pixel) che l'applet può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli Applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applet vengano lanciati sul client, essi non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Client mail

Un client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne nel computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico

Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendole cedere informazione privata che verrà usata per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto

in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina Web è finta, e organizzata soltanto per rubare l'informazione del utente.

Virus polimorfico
Virus che modifica la propria forma con ogni file che infetta. In quanto non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.

Porta
Interfaccia su un computer alla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modem, delle stampanti, dei mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di report
File che elenca le azioni avvenute. BitDefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e file esaminati, quanti file infetti e sospetti sono stati trovati.

Rootkit
Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento.

Script
Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiasi e-mail non richiesta.

Spyware

Accede alla connessione internet dell'utente senza che l'utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware vengono tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare una vittima dello spyware è scaricare certi file peer-to-peer scambiando prodotti che sono disponibili oggi.

A parte delle questioni dell'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer “mangiandosi” larghezza di banda dal momento in cui invia informazione alla sua “casa” usando l' internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra delle applicazioni è situata nella barra degli strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio clic o fare clic con il pulsante destro su un'icona per vedere ed accedere ai dettagli e ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario introduce i virus nel vostro computer.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e catturare Troia.

Aggiorna

La nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

BitDefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer senza che voi lo sappiate e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.